625-CD-604-001

EOSDIS Core System Project

ECS Project Training Material
Volume 4: System Administration

March 2001

Raytheon Company
Upper Marlboro, Maryland

ECS Project Training Material
Volume 4: System Administration

March 2001

Prepared Under Contract NAS5-60000
CDRL Item 129

RESPONSIBLE ENGINEER

Michael B. Blumenthal 3/7/01

Michael J. Blumenthal Date
EOSDIS Core System Project

SUBMITTED BY

Gary W. Sloan /s/ 3/8/01

Gary Sloan, M&O Manager Date
EOSDIS Core System Project

Raytheon Company
Upper Marlboro, Maryland

This page intentionally left blank.

Preface

This document is a contract deliverable with an approval code of 3. As such, it does not require formal Government approval. This document is delivered for information only, but is subject to approval as meeting contractual requirements.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Company
1616 McCormick Dr.
Upper Marlboro, MD 20774-5372

Note: This document contains change bars to indicate the addition or revision of material since the issuance of the predecessor document containing training material for Release 5B of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS).

This page intentionally left blank.

Abstract

This is Volume 4 of a series of lessons containing the training material for Release 5 of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the process required for submitting and updating trouble tickets as well as investigating problems and identifying and implementing solutions.

***Keywords**:* training, instructional design, course objective, problem management, trouble ticket, trouble ticket review board, failure review board, Remedy.

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Original
iii through xii	Original
1 through 86	Original
Slide Presentation 1 through 72	Original

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
625-CD-604-001	Original	March 2001	

This page intentionally left blank.

Contents

Secure Shell (ssh)

System Startup and Shutdown

System Software Server Failover/Dependencies

Checking the Health and Status of the System

Tape Operations

System Backups and Restores

System Log Maintenance

User Administration

Commercial Off-the-Shelf (COTS) Administration

Security

Practical Exercises

Slide Presentation

Introduction

Identification

Training Material Volume 4 is part of Contract Data Requirements List (CDRL) Item 129, whose requirements are specified in Data Item Description (DID) 625/OP3 and is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-60000).

Scope

Training Material Volume 4: System Administration defines the steps required to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding Network Administration. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Status and Schedule

This lesson module provides detailed information about training for Release 5. Subsequent revisions will be submitted as needed.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Related Documentation:	Related Documentation identifies parent, applicable and information documents associated with this document.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

Related Documentation

Parent Document

The parent document is the document from which this ECS Training Material's scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work

Applicable Documents

The following documents are referenced within this ECS Training Material, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)

Information Documents

Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

609-CD-600	Release 6A Operations Tools Manual for the ECS Project
611-CD-600	Mission Operation Procedures for the ECS Project
910-TDA-022	Custom Configuration Parameters for ECS Release 6A

Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

305-CD-600	Release 6A Segment/Design Specification for the ECS Project
311-CD-600	Release 6A Data Management Subsystem Database Design and Database Schema Specifications for the ECS Project
311-CD-601	Release 6A Ingest Database Design and Database Schema Specifications for the ECS Project
311-CD-602	Release 6A Interoperability Subsystem (IOS) Database Design and Database Schema Specifications for the ECS Project

311-CD-603	Release 6A Planning and Data Processing Subsystem Database Design and Schema Specifications for the ECS Project
311-CD-604	Release 6A Science Data Server Database Design and Schema Specifications for the ECS Project
311-CD-605	Release 6A Storage Management and Data Distribution Subsystems Database Design and Database Schema Specifications for the ECS Project
311-CD-606	Release 6A Subscription Server Database Design and Schema Specifications for the ECS Project
311-CD-607	Release 6A Systems Management Subsystem Database Design and Schema Specifications for the ECS Project
311-CD-608	Release 6A Registry Database Design and Schema Specifications for the ECS Project
313-CD-600	Release 6A ECS Internal Interface Control Document for the ECS Project
334-CD-600	6A Science System Release Plan for the ECS Project
601-CD-001	Maintenance and Operations Management Plan for the ECS Project
603-CD-003	ECS Operational Readiness Plan for Release 2.0
604-CD-001	Operations Concept for the ECS Project: Part 1-- ECS Overview
604-CD-002	Operations Concept for the ECS Project: Part 2B -- ECS Release B
605-CD-002	Release B SDPS/CSMS Operations Scenarios for the ECS Project
607-CD-001	ECS Maintenance and Operations Position Descriptions
152-TP-001	ACRONYMS for the EOSDIS Core System (ECS) Project
152-TP-003	Glossary of Terms for the EOSDIS Core System (ECS) Project
211-TP-005	Transition Plan 4PX to 4PY, 4PY to 5A, and 5A to 5B for the ECS Project
220-TP-001	Operations Scenarios - ECS Release B.0 Impacts
500-1002	Goddard Space Flight Center, Network and Mission Operations Support (NMOS) Certification Program, 1/90
535-TIP-CPT-001	Goddard Space Flight Center, Mission Operations and Data Systems Directorate (MO&DSD) Technical Information Program Networks Technical Training Facility, Contractor-Provided Training Specification

System Administration

Lesson Overview

This lesson will provide you with the tools needed to perform the various tasks required to administer Implementation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations.

Lesson Objectives

Overall Objective - The overall objective of his lesson is proficiency in the various tasks required to administer the ECS during maintenance and operations.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will use the Procedures Manual in accordance with prescribed methods and complete required procedures without error to accomplish all tasks required.

Specific Objective 1 - The student will perform a Secure Shell login to ECS and.establish a personal passphrase

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to login to ECS using Secure Shell and establish a personal passphrase.

Specific Objective 2 - The student will manually shutdown and restart a single subsystem of the ECS without affecting other subsystems.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems from the command line.

Specific Objective 3 - The student will shutdown and restart a single subsystem of the ECS using ECS Assistant without affecting other subsystems.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems using the ECS Assistant.

Specific Objective 4 - The student will start the Tivoli Management Environment monitoring program.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to start the Tivoli Management Environment monitoring program.

Specific Objective 5 - The student will determine the active monitor profiles for any specific ECS host using the Tivoli Management Environment.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to determine which monitor profiles are active for any specific ECS host using the Tivoli Management Environment.

Specific Objective 6 - The student will be able to label and index a tape cartridge.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to label a tape and index a tape cartridge.

Specific Objective 7 - The student will be able to create an incremental tape backup.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to create an incremental tape backup of system files created or modified within the past six days.

Specific Objective 8 - The student will be able to create a tape backup of the entire ECS system.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform a complete tape backup of the ECS.

Specific Objective 9 - The student will be able to restore individual files or entire volumes of backup tapes to the ECS system.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform individual or complete file restorations.

Specific Objective 10 - The student will be able to review and modify system logs.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform system log maintenance.

Specific Objective 11 - The student will create, modify, and delete user accounts on the ECS.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to add a new user account to the ECS, make modifications to a variety of account access parameters, and delete the account from the ECS.

Specific Objective 12 - The student will be able to check and modify access privileges on files and directories across the ECS.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to check file and directory access privileges and modify them to allow or deny access by various classes of users.

Specific Objective 13 - The student will be able to determine when security breaches occur and will be able to remedy such breaches.

Condition - The student will be given a copy of *625-CD-604-001ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to identify when security breaches occur and to remedy such breaches.

Importance

A System Administrator's goal is to keep the computer system usable by the users. A system running at peak efficiency does so because of the proper use of the tools provided for and used by the System Administrator. Intimate knowledge of how each tool works and which should be used in a particular situation is crucial to satisfying the ECS user community.

This page intentionally left blank.

Secure Shell (ssh)

In this lesson you will learn how Secure Shell is used to make the ECS working environment more secure by using the Secure Shell (**ssh**) and Secure Login (**slogin**) commands to access ECS.

What is Secure Shell?

Secure Shell (ssh) is a set of programs that greatly improve network security. The primary need for it on ECS is to allow secure, interactive access to ECS DAACs without needing burdensome procedures and mechanisms and additional hardware.

Secure in this context means not sending passwords "in the clear" so that hackers may intercept them and also provides encryption of the entire session.

Secure Access to ECS DAACs

ECS has implemented a Local Area Network (LAN) at the DAACs that is more secure than most other LANs. From the Internet, it is not possible to directly connect with all hosts at a DAAC. There is a set of hosts that are "dual-homed" to a user LAN that is connected on one side to the Internet and to the DAAC production LAN on the other side. This will require an interactive user to first use ssh to access a dual homed host and then use ssh to access a production host. In order to minimize the impact on the user, a single login has been implemented.

Setting Up ssh

Ssh programs have client and server components much like other network programs. The user only needs to be concerned with the client configuration as the server side is set up by a systems administrator. The amount of effort that it takes to get ssh going depends on how many different home directories the user has. At Landover, for instance, there are separate directories for the EDF and the VATC.

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing ssh commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via ssh. The process is started by running the sshsetup script which will enable ssh to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

Initiating sshsetup procedure

1 Login to your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup**, then press Return/Enter.

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

Initializing random number generator...

Generating p: Please wait while the program completes ...

%

- This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.

Remote ssh Access

If you need to access a host with a different home directory, you will need to run the sshremote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

Setting up remote access ssh procedure

1 Login into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote**, then press Return/Enter.

- You will see the following prompt:

You have a local passphrase. Do you want to setup for:

1 VATC

2 EDF

3 MiniDAAC

4 GSFC DAAC

5 GSFC M and O

6 EDC DAAC

7 EDC M and O

8 LaRC DAAC

9 LaRC M and O

10 NSIDC DAAC

11 NSIDC M and O

12 Exit from script

Select:

3 At the "Select" prompt, type in the corresponding number to the desired host, then press Return/Enter.

- You will receive a prompt similar to the following for the VATC:

Working...

4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** and then press Return/Enter.

- A prompt similar to the following will be displayed:

Last login: Thu Jul 9 10:41:13 1998 from echuser.east.hit

No mail.

Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996

t1code1{username}1:

5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

Initializing random number generator...

Generating p: Please wait while the program completes ...

%

8 At the "t1code1" prompt type **exit**, the press Return/Enter.

- The following information will be displayed:

Updating locally...

Updating t1code1u.ecs.nasa.gov

%

- This establishes the ssh key at the remote host and exchanges key information with your local host.

Note: The ssh keys at remote sites can be different from the local host ssh key.

Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The ssh keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

Changing Your Passphrase Procedure

1 Login to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **/tools/bin/sshchpass**, then press Return/Enter.
- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see an information prompt similar to the following:

ssh-keygen will now be executed. Please wait for the prompt to Return!

/home/bpeters/.ssh/authorized_keys permissions have already been set.

%

System Startup and Shutdown

Overview

Starting or shutting down a computer system may involve nothing more than turning a power switch to the on or off position. However, the interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

A complete system startup and shutdown should only need to occur approximately once in three or four months during the early stages of system implementation due to the inherent instability of new systems. After the system stabilizes, it is estimated that complete system startups and shutdowns will occur only about once a year. Partial shutdowns and restarts will be performed as needed due to maintenance concerns.

Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, such as when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off, or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

The Cold System Startup is done in sequential order by subsystem. Figure 1 below shows the order at the DAAC in which each server is to be booted to achieve a fully functional system.

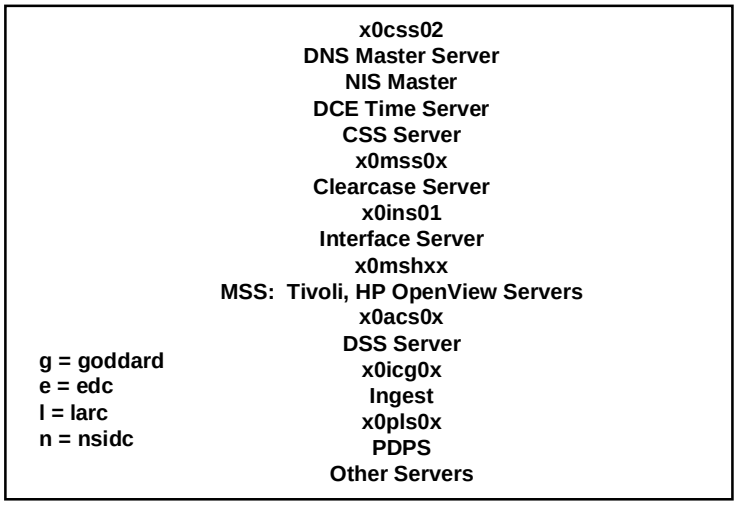

Figure 1. DAAC Server Startup Order

Cold Subsystem Startup Procedure

1 Determine which machines perform the following functions. Some may perform multiple functions:

- Domain Name Server (DNS) Master
- Name Information Server (NIS) Master
- Mail Hub Server(s)
- Automount Servers
- Clearcase Server
- Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server
- DCE License Server for SUN
- Other License Servers
- Sybase SQL Servers
- Data Server Subsystem (DSS)
- Planning & Data Processing System (PDPS)
- Client, Interoperability and Data Management (CIDM) Subsystem

2 Startup the DNS Master, the NIS Master, the DCE Time server and the CSS server. Once that system has booted without error, proceed to step 3.

3 Power on the Clearcase server(s). Once the systems(s) have booted without error, proceed to step 4.

4 Power on the Interface server(s). Once the system(s) have booted without error, proceed to step 5.

5 Power on the MSS server(s). Once the system(s) have booted without error, proceed to step 6.

6 Power on the DSS server(s). Once the system(s) have booted without error, proceed to step 7.

7 Power on the Ingest server(s). Once the system(s) have booted without error, proceed to step 8.

8 Power on the PDPS server(s). Once the system(s) have booted without error, proceed to step 9.

9 Power on the Client, Interoperability and Data Management CIDM server(s).

Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

Warm Subsystem Startup Procedure

1 Determine which machines perform the following functions:

- Domain Name Server (DNS) Master
- Name Information Server (NIS) Master
- Mail Hub Server(s)
- Automount Servers
- Clearcase Server
- Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server
- DCE License Server for SUN
- Other License Servers
- System Management Subsystem
- Sybase SQL Servers
- Data Server Subsystem (DSS)
- Planning & Data Processing System (PDPS)
- Client, Interoperability and Data Management (CIDM) Subsystem

2 Determine which machine is currently down.

3 Determine the interoperability dependencies among the machines.

4 Turn on machines in an order consistent with the dependencies.

Note - in addition to warm system startup/reboot sequences, ECS servers which use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted, once the Sybase SQL server has come back on-line.

Additional tasking - Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Program Generated Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are ${PGSHOME}/database/common/TD/leapsec.dat and ${PGSHOME}/database/common/CSC/utcpole.dat. The update of these files is accomplished by executing leapsec_update.sh and utcpole_update.sh in the /tools/admin/exec directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting.

Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. Normal shutdowns are scheduled by the Resource Manager with prior approval by the DAAC management at a time that minimizes disruption to system users, usually during off hours. No loss of data is anticipated from a normal shutdown. All subsystems are shutdown in a routine and normal fashion.

The system shutdown procedure is performed by the System Administrator at the discretion of the Network Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup. Figure 2 below shows the order at the DAAC in which each server is to be shutdown to achieve an orderly shutdown.

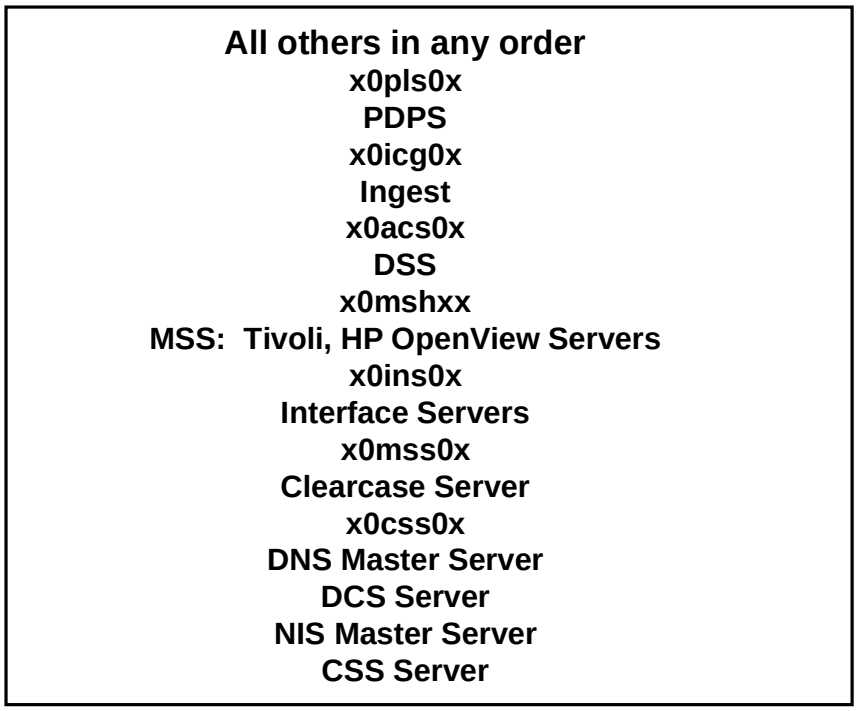

Figure 2. DAAC Server Shutdown Order

The System Administrator must be logged in as root to perform a shutdown.

Prior to a normal shutdown, the System Administrator sends broadcast messages to all Computer Operators on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and Shutdown Minus 1 minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems in the order prescribed in the procedure below.

HP OpenView is used as the monitoring agent with each subsystem icon turning red as it is successfully shutdown. When all subsystems have been successfully shutdown, the UNIX prompt appears on the console screen. Total time from shutdown initiation to completion may be as long as 45 minutes.

Normal Shutdown By Subsystem Procedure

Steps A-G below are preliminary steps to shutting down each subsystem.

A Login to the server as **root**.

B Enter root password.

C Type **wall** and press **Return/Enter**.

D Type **This machine is being shutdown for *reason*. Please save your work and log off now. We are sorry for the inconvenience.** Press Control and D keys simultaneously.

E Wait at least five minutes.

F Type **shutdown -g0 -i0** or **shutdown now -i0** at the UNIX prompt and press **Return/Enter**.

G Power off all peripherals and the CPU.

1 Determine which machines perform the following functions:

- DNS Master
- NIS Master
- Mail Hub Server(s)
- Automount Server
- Clearcase Server
- CSS including DCE Server
- DCE License Server for SUN
- Other License Servers
- MSS including Tivoli Server and Sybase SQL Servers
- DSS
- Ingest
- PDPS
- CIDM

2 Power off the CIDM server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 3.

3 Power off the PDPS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 4.

4 Power off the Ingest server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 5.

5 Power off the DSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 6.

6 Power off the MSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 7.

7 Power off the Interface server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 8.

8 Power off the Clearcase server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 9.

9 Power off the CSS server, the DCE Time server, the NIS Master and the DNS Master by following steps A-G above for each machine

Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- the system or subsystem is locked up and users are unable to access or maneuver through the system
- an impending or actual power failure
- an actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

If the entire system is locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If major subsystems are locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are impacted, the subsystem problem(s) should be resolved first. If after all efforts to resolve the subsystem problems are exhausted the System Administrator determines that a shutdown is necessary, only those affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made not to impact users that are still on the system and to minimize data loss.

Emergency Shutdown Procedure

1 Login to the server as root.

2 Enter root password.

3 Type **sync** at the UNIX prompt, then press **Return/Enter**.

- **sync** causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, sync must be called to insure file system integrity.

4 Type **sync** again at the UNIX prompt, then press **Return/Enter**.

5 Type **halt** at the UNIX prompt, then press **Return/Enter**.

6 Shutdown all client workstations.

7 Determine which machines perform the following functions. Some machines may perform multiple functions:

- Sybase SQL/Rep
- Autosys
- Clearcase
- Tivoli
- DCE
- Automount
- Mail Hub
- NIS
- DNS

8 Power off the Sybase SQL/Rep server(s). Once the system has shutdown without error, proceed to Step 9.

9 Power off the Autosys server(s). Once the system has shutdown without error, proceed to Step 10.

10 Power off the Clearcase server(s). Once the system has shutdown without error, proceed to Step 11.

11 Power off the Tivoli server(s). Once the system has shutdown without error, proceed to Step 12.

12 Power off the DCE server(s). Once the system has shutdown without error, proceed to Step 13.

13 Power off the Automount server(s). Once the system has shutdown without error, proceed to Step 14.

14 Power off the NIS server(s). Once the system has shutdown without error, proceed to Step 15.

15 Power off the DNS server(s).

In case of EXTREME emergency where time does not allow you to execute the above procedures, execute the procedure steps that follow. Be forewarned, however, that this procedure does not ensure file system integrity and will result in loss of data and/or damage to the file system. It should be used only as a last resort.

Extreme Emergency System Shutdown Procedure

1 At the **Login:** prompt, type **root,** then press **Return/Enter**.

2 At the **Password:** prompt, enter the ***RootPassword***.

3 Press the **L1** and the **a** keys simultaneously.

4 Once returned to an **ok** or **>** prompt, turn the power switches on the CPU and all peripherals to the **off** position.

WARNING

The use of L1-a does not ensure file system integrity. There is a very high risk of losing data when this process is used.

System Shutdown by Server

In situations where only a single server requires maintenance the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.

System Software Server Failover/Dependencies

Overview

In addition to the hardware aspect of server startup and shutdown, ECS has a unique concept of software servers that also have their own hierarchical dependencies for startup and shutdown sequencing. Ingest servers such as EcInGran, EcInReqMgr, and EcInMailGWServer and Science Data Servers such as EcDsScienceDataServer and EcDsHdfEosServer, have fault recovery aspects and server sequencing aspects that must be taken into consideration during system monitoring and administration.

Updates to this section will cover those software server dependencies and failover design features and provide procedures to ensure optimum system operation.

This page intentionally left blank.

Checking the Health and Status of the System

System Monitoring Tools

Whazzup???

A powerful COTS program modified for ECS and used to monitor the ECS system is EcMsWz - Whazzup. It is a web accessed program that provides a graphical display of Host Status, Mode Status, Mode Verification and Performance Management. Figure 3 shows the initial Whazzup display.

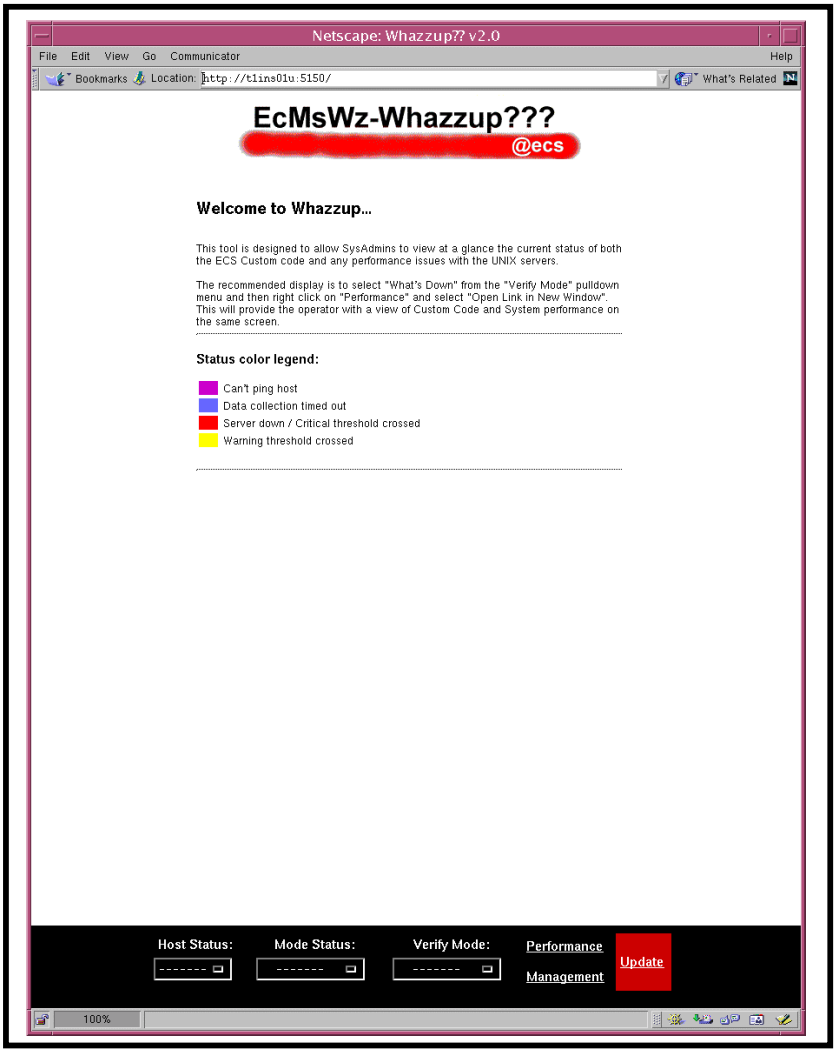

Figure 3. ECS Whazzup initial display

These functions of Whazzup provide graphical displays of host and software-server status in real-time mode. When used in conjunction with Tivoli and ECS Assistant, System Administrators can acquire a comprehensive knowledge of the system's status.

To start EcMsWz-Whazzup, execute the procedure steps that follow:

Logon onto a host machine

2 At the UNIX prompt on the host from which Whazzup is to be run, type **setenv DISPLAY <hostname>:0.0**, press **Return/Enter**. Note: If the host has been remotely accessed via ssh then do not use the setenv DISPLAY command again. Doing so will compromise system security.

- The hostname is the name of the machine on which Whazzup is to be displayed, i.e., the machine you are using.

- To verify the setting, type **echo $DISPLAY**, press **Return/Enter**.

3 At the UNIX prompt, using secure shell, log on to the Whazzup host, xxins0x. Type **ssh xxins0x**, press **Return/Enter**. Enter your **passphrase**, press **Return/Enter**.

- You are logged into the Whazzup host machine.

4 Start the Netscape web browser by typing **netscape &**, press **Return/Enter.**

- You are in the web browser on the Whazzaup host xxins0x.

5 Type in the URL to activate Whazzup. Enter **http://xxins0x:5150**.

- The Whazzup intro screen appears (Figure xx).

6 Select a monitoring function

- **Host Status** to determine individual host parameters.
- **Mode Status** to determine "up" servers for the selected Mode.
- **Verify Mode** to determine status of all servers for a selected Mode.
- **Performance Management** to determine the performance status all hardware/software servers for all modes.

Host Status

Selecting Host Status provides a pop-up box (Figure 4) from which to choose a specific host to determine its status.

Figure 4. Host Status pop-up display

Host Status data include percent of CPU used, Swap Free space, Memory Free space, and Server information. (Figure 5)

Figure 5. Host Status data displayMode Status

Selecting Mode Status (Figure 6) enables a pop-up window showing Modes available. Subsequent to selecting the desired Mode, a display of "up" ECS Servers is provided as shown in Figure 7.

Figure 6. Mode Status pop-up display

Figure 7. Mode Status data display

Verify Mode

Selecting **Verify Mode** and choosing a desired mode (Figure 8) will provide a thorough display of ECS server status, by host, for the mode (Figure 9). Alternatively, selecting **What's Down** will provide a display indicating all down ECS servers, by mode, by host.

Figure 8. Verify Mode pop-up display

Figure 9. Verify Mode data display

Performance Management

Following recommended monitoring procedures, the optimum method of system monitoring is to select **What's Down** from **Verify Mode** and then **Right Click** on **Performance Management** (Figure 10) and open the link in a new window (Figure 11).

Figure 10. Performance Management selection display

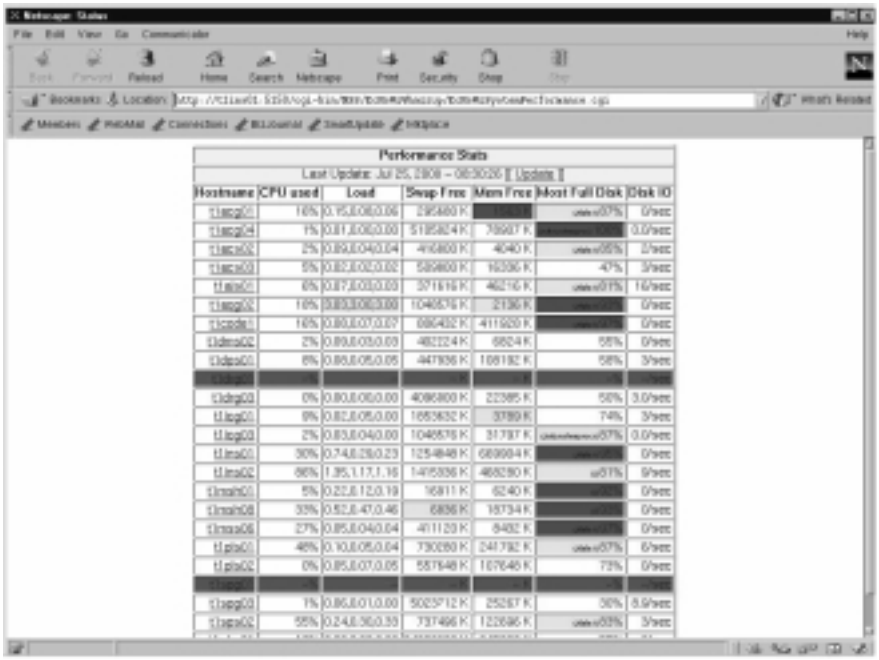

Figure 11. Performance Management data display

Having these two displays active simultaneously will provide the Systems Administrator the status of "down" ECS servers and the performance status of individual hosts.

ECS Assistant and ECS Monitor

The Whazzup tool provides a quick look capability to note whether any servers are down. The ECS Assistant and ECS Monitor tools provide additional easy-to-use tools that offer a server monitoring and ping capability (ECS Monitor) as well as a capability to start and stop servers (ECS Assistant). Figure 12 shows the ECS Assistant GUI for access to manager functions, the ECS Assistant subsystem manager GUI, and an example of a confirmation dialog.

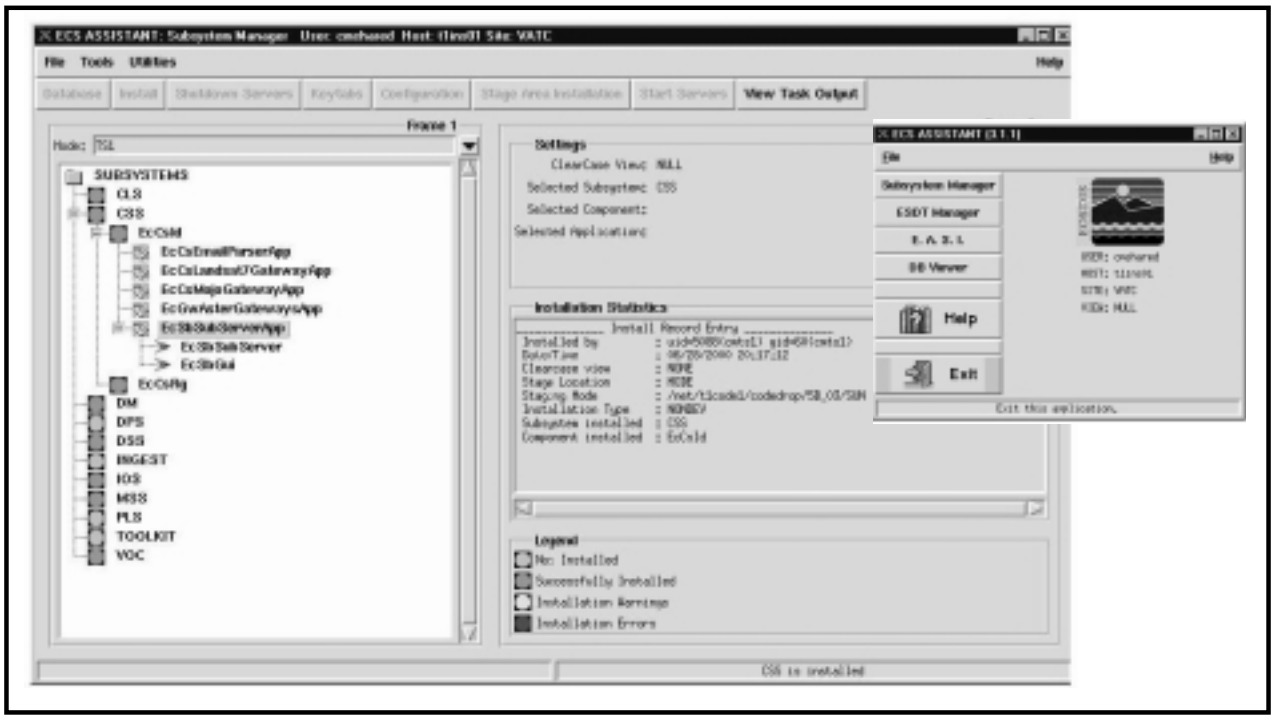

Figure 12. ECS Assistant GUI Manager Windows

To run the ECS Assistant, use the following procedure.

Starting ECS Assistant

1 Log in to one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, and then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME**, and then press the **Return/Enter** key.

3 At the UNIX prompt, type **cd /tools/common/ea**, and then press the **Return/Enter** key. Then type **EcCoAssist /tools/common/ea &**, and then press the **Return/Enter** key.

- **/tools/common/ea** is the path where ECS Assistant is installed, and also where EcCoScriptlib may be found.
- The ECS Assistant GUI is displayed.

4 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- The Subsystem Manager GUI is displayed.

5 Select a mode by clicking on the down arrow at the right end of the **Mode** field and then on the desired mode name in the resulting list.

- The selected mode is displayed in the **Mode** field and colored indicators show the installation status for components in that mode on the host; the legend for the color indications is at the lower right on the Subsystem Manager window.

6 In the list of subsystems, double click on the name of the subsystem of interest.

- One or more component groups appear below the selected subsystem name.

7 Double click on the name of a component group.

- One or more application groups appear below the selected component group name.

8 Double click on the name of the application group of interest.

- The applications or servers in the selected group are listed below the name of the group.

9 Single click on the name of an application or server of interest.

- The selected application or server is highlighted.
- Detailed installation information is displayed in the **Installation Statistics** window.

ECS Monitor provides a convenient way to monitor the status of the servers by listing their up/down condition. The **ECS Monitor** GUI is shown in Figure 13; the status flag for a server is up or down indicating whether or not that server is running, and for a server that is running, the window shows the process ID (PID), the user ID, and the start time. The ECS Monitor also includes near the top of the window a button labelled **cdsping all servers . . .** that permits an operator to ping all servers. Figure 14 shows the resulting **ECS Monitor cdsping** window.

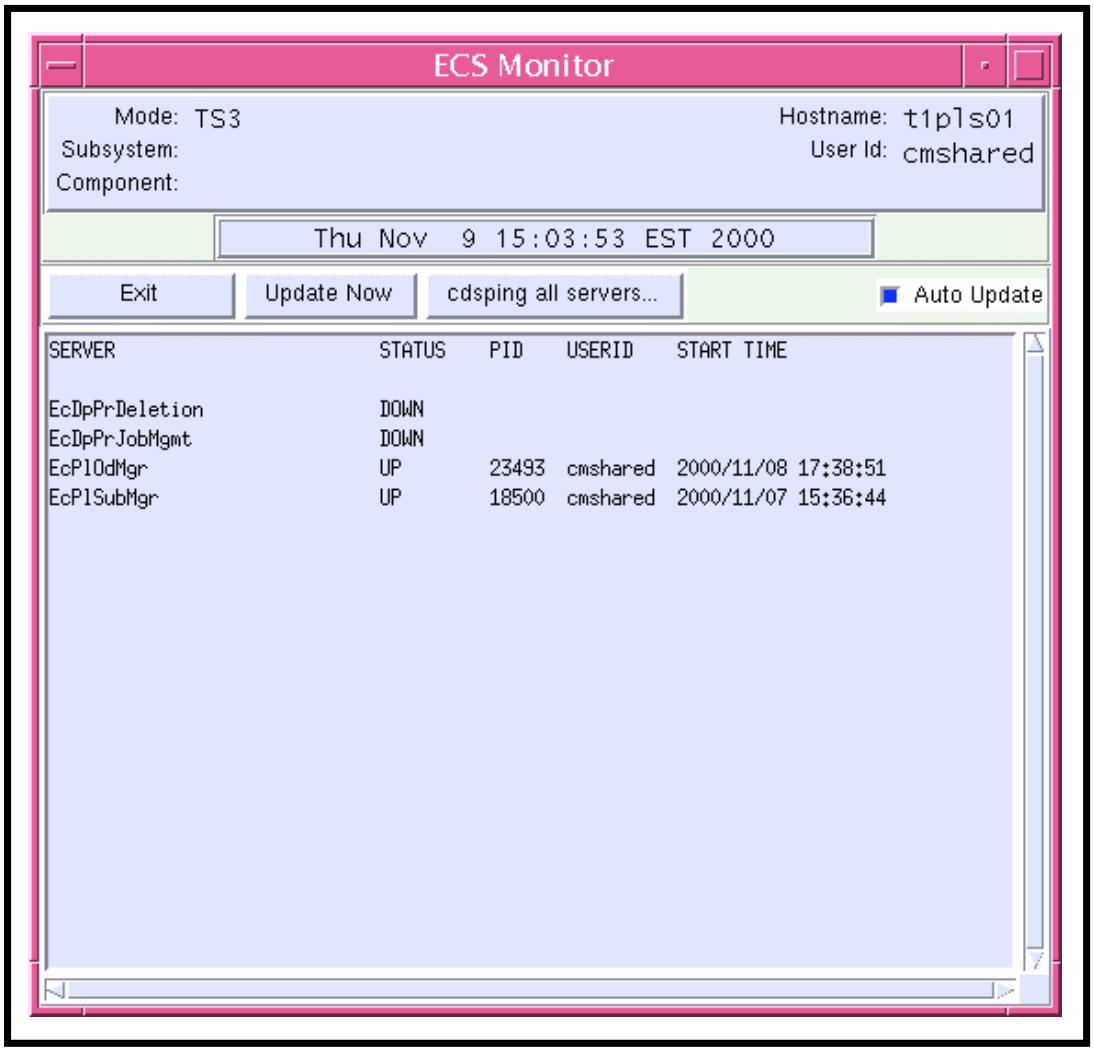

Figure 13. ECS Monitor GUI

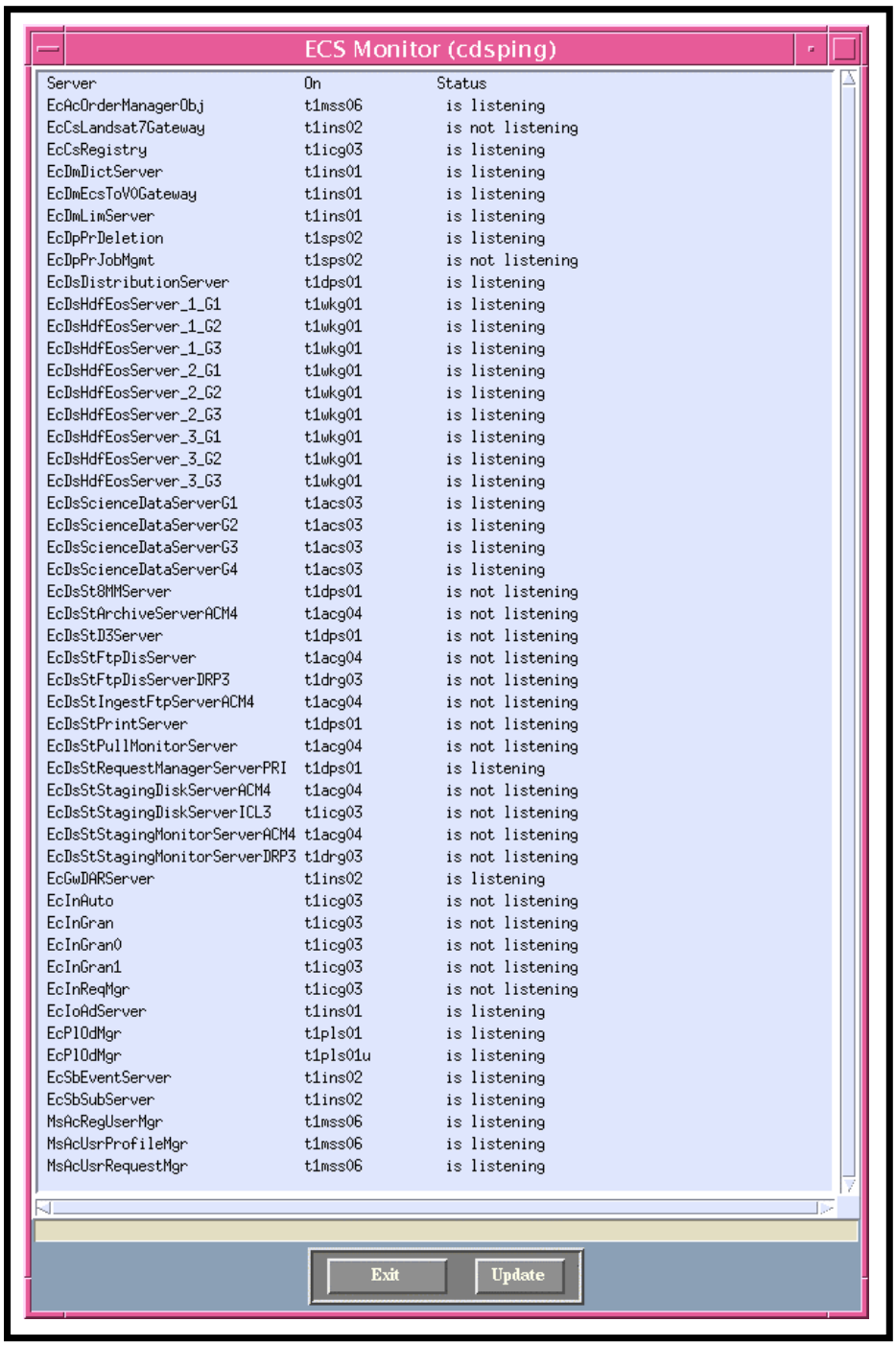

Figure 14. ECS Monitor cdsping GUI

To start up the ECS Monitor GUI, use the following procedure.

Using the ECS Assistant Server Monitor

1 Log in to one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, and then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME**, and then press the **Return/Enter** key.

3 At the UNIX prompt, type **cd /tools/common/ea**, and then press the **Return/Enter** key.

- **/tools/common/ea** is the path where ECS Monitor is installed.

4 Then type **EcCoMonitorGui /tools/common/ea <*mode*> &**, and then press the **Return/Enter** key.

- **/tools/common/ea** is the path where EcCoScriptlib may be found.
- The **ECS Monitor GUI** is displayed, showing the status (**UP** or **DOWN**) of the servers on the current host in the mode specified in the command, as indicated near the top left corner of the window.
- The status "**UP/DOWN**" indicates whether a listed server is running.

5 To see which host each server is running on, click the **cdsping all servers…** button.

- The **ECS Monitor (cdsping)** GUI is displayed.
- The host name for each running server is listed, and whether or not it is listening.

6 Both the **Server Monitor** and **cdsping** GUI can be updated by clicking the **update** button in the GUI.

- This causes the list to update to the current status.

7 To monitor other servers, log in to other hosts and launch the ECS Monitor GUI in the desired mode, as in steps 2-4.

To exit, click the **EXIT** button.This terminates display of the monitor GUI.

Tivoli Management Environment

Another powerful COTS program used to monitor the system is Tivoli Management Environment. Version 3.6 is the current version installed at the DAACs. Tivoli is based on a core program, Tivoli Framework, to which specific user applications are added to meet management and monitoring requirements. These applications, when configured for specific ECS functions, provide detailed information and notification of events on a programmable polling basis.

Specific Tivoli Environment applications used in ECS are:

- Tivoli Enterprise Console. A rules-based management application that collects, processes, and automatically responds to common management events.
- Tivoli Software Distribution (previously Tivoli Courier). A management application that provides for the distribution and installation of software on machines in a heterogeneous networking computing environment.
- Tivoli Distributed Monitoring (previously Tivoli Sentry). A management application for monitoring system and application resources and generating events and alarms on a network-wide basis. It provides availability data and performs automated actions based on the monitored data.

Tivoli Management Environment, when used in conjunction with Whazzup??? and ECS Monitor, can provide detailed, current data on system status. *Figure 15* depicts the component relationship of Tivoli Management Environment and the three applications used in ECS.

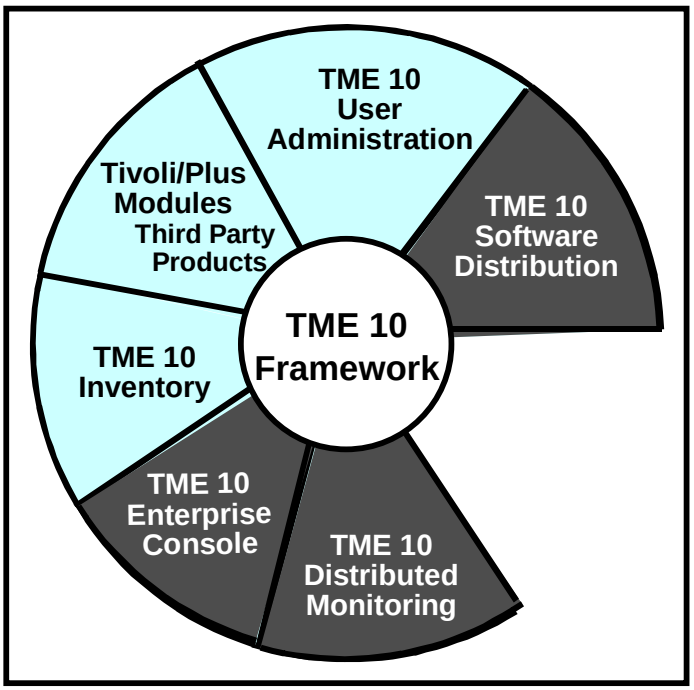

Figure 15. Tivoli Management Enterprise Components

Tivoli Management Region

The core of a Tivoli Management Environment is the Tivoli Management Region, or TMR. It consists physically of a primary Server and its clients. In ECS, the TMR is normally installed on the MSS Server. As an example, for GSFC, it is located on g0msh08, and for the VATC it is installed on t1msh01.

Complete installation instructions and release notes for Tivoli Management Environment, Version 3.6 Upgrade for the ECS Project, are contained in the ECS Project document 914-TDA-043-REV01.

The program is accessed by various levels of administrators. During installation, the installer assumes the highest level of administrator, the Super Administrator. After installation, other administrators are created and provided specific authorization roles as required, such as Senior, Admin, and User. Administrators can only create other administrator accounts that have capabilities equal to, or less than, their own level.

Figure 16 illustrates the Tivoli Startup screen, which appears briefly upon starting the program. The Administrator Desktop, illustrated in Figure 17, is displayed immediately after the appearance of the Startup screen. As shown in Figure 17 the Desktop screen features icons which permit access to various administrative functions.

Figure 16. Tivoli Startup Screen

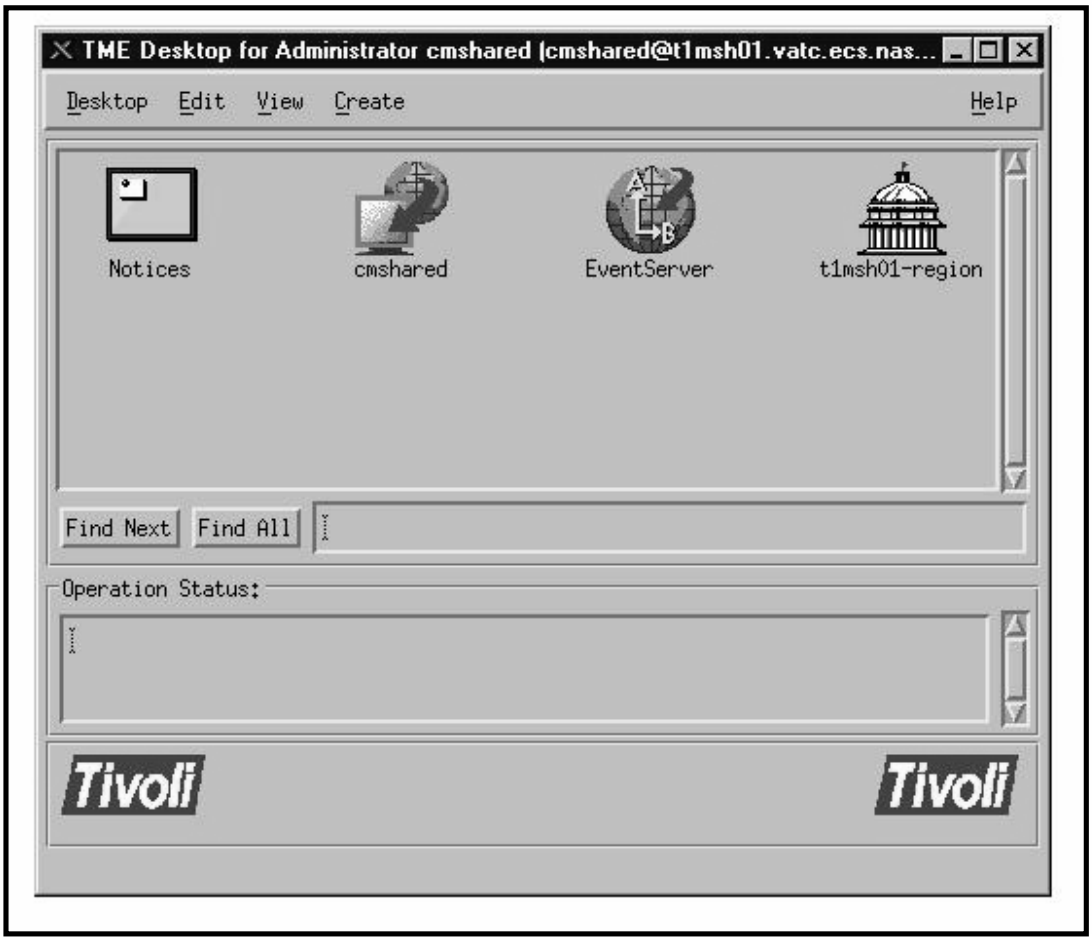

Figure 17. Tivoli TME Administrator Desktop

To run Tivoli, execute the procedure steps that follow:

Tivoli startup procedure

1 Log in to a host machine.

2 At the UNIX prompt on the host from which Tivoli is to be run, type **setenv DISPLAY hostname:0.0** and the press the **Return/Enter** key. ***Note***: If the host has been remotely accessed via ssh then do not use the setenv DISPLAY command again. Doing so will compromise system security.

- The hostname is the name of the machine on which Tivoli is to be displayed, i.e., the machine you are using.
- To verify the setting, type **echo $DISPLAY** and then press the **Return/Enter** key.

3 At the UNIX prompt, using secure shell, log on to the Tivoli host, *x*0msh*xx*. Type **ssh *x*0msh*xx*** and then press the **Return/enter** key. Enter <***your passphrase***> and then press the **Return/Enter** key.

- You are logged into the Tivoli host machine.

4 Type **cd /etc/Tivoli** and then press the **Return/Enter** key.

- You are in the Tivoli directory on host ***x*0msh*xx***.

5 Type **source setup_env.csh** and then press the **Return/Enter** key.

- The environment variables for Tivoli are set.

6 Type **tivoli –f** and then press the **Return/Enter** key.

- The Tivoli Startup screen appears briefly, followed by the TME Administrator Desktop.

Tivoli Policy Region

Monitoring of system resources uses displays that are organized analogous to a hierarchical file structure. Accessed through the top-level policy region icon, displayed on the Administrator Desktop (Figure 17), subsequent screens display specific hosts and agents. A policy region is a special collection of resources that share one or more common policies. An administrator can create special sub-policy regions to monitor specific areas of interest. Policy sub-regions can be arbitrarily nested and can contain any desired set of managed resources.

Figure 18 and Figure 18a show the Policy Region content for the VATC system under TMR t1msh01. It has been populated with the individual hosts and other managed resources under Tivoli management purview.

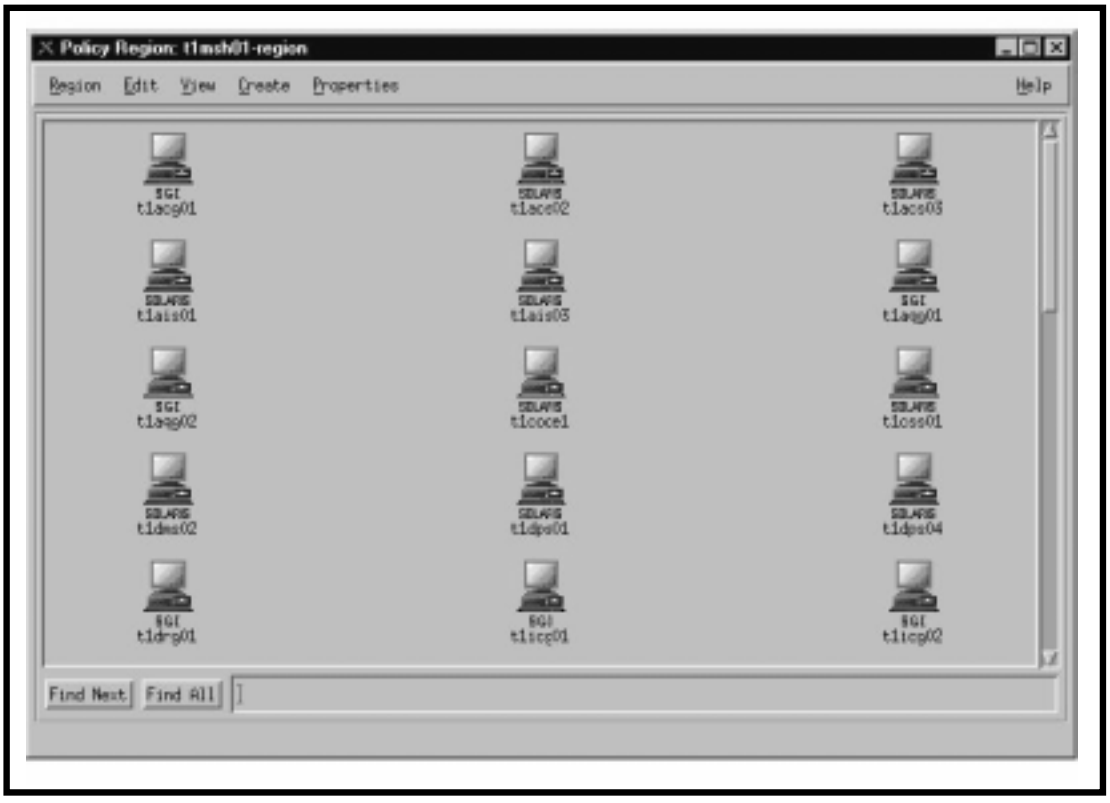

Figure 18. Policy Region content for t1msh01 in the VATC

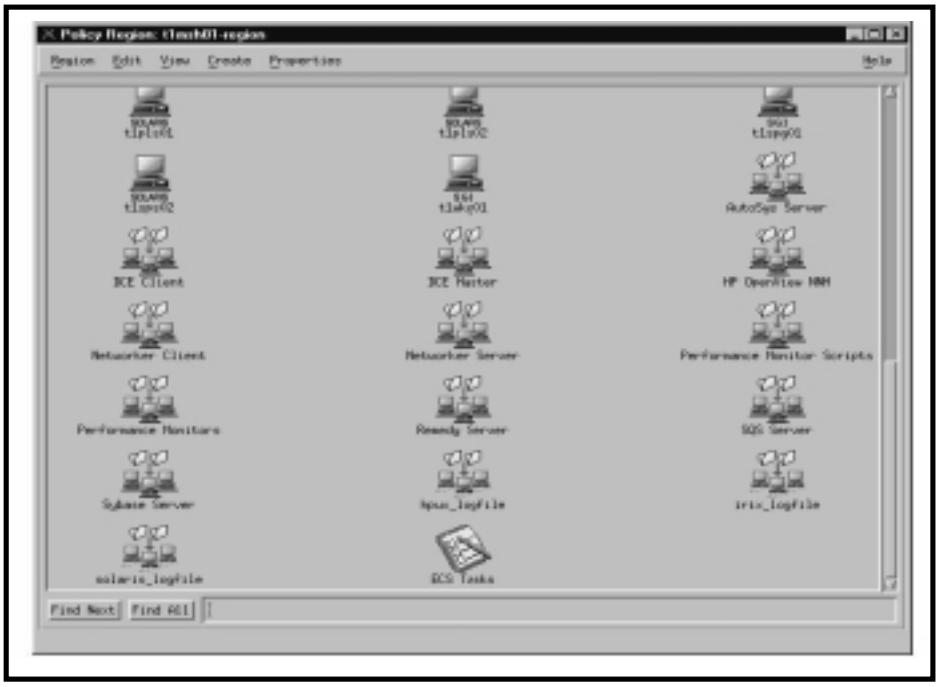

Figure 18a. **Policy Region content for t1msh01 in *the VATC, continued***

Distributed Monitoring

The component of Tivoli Management Environment that establishes system monitoring criteria is the Tivoli Distributed Monitoring application. Tivoli Distributed Monitoring checks the status of a variety of networked resources, such as systems, applications, and processes. Through the use of profiles, Distributed Monitoring enables system administrators to set monitoring policy and to change monitoring parameters for any number of related, remote systems from a single location. Distributed Monitoring profiles also define automated responses. These responses can be as simple as changing the status of an icon or sending E-mail to an administrator, or as complex as sending an SNMP trap or running a user-specified program or script.

Key items that can be set for any given monitor are:

- Set the response level.
- Determine monitor trigger.
- Send a Tivoli Notice.
- Activate a Pop-up Window.
- Change an icon's status.

Send E-mail.

- Log to a file.
- Run a program.

An example of a monitor profile is shown in Figure 19. It is the profile edit screen establishing a Daemon Monitor on the VATC host t1msh01.

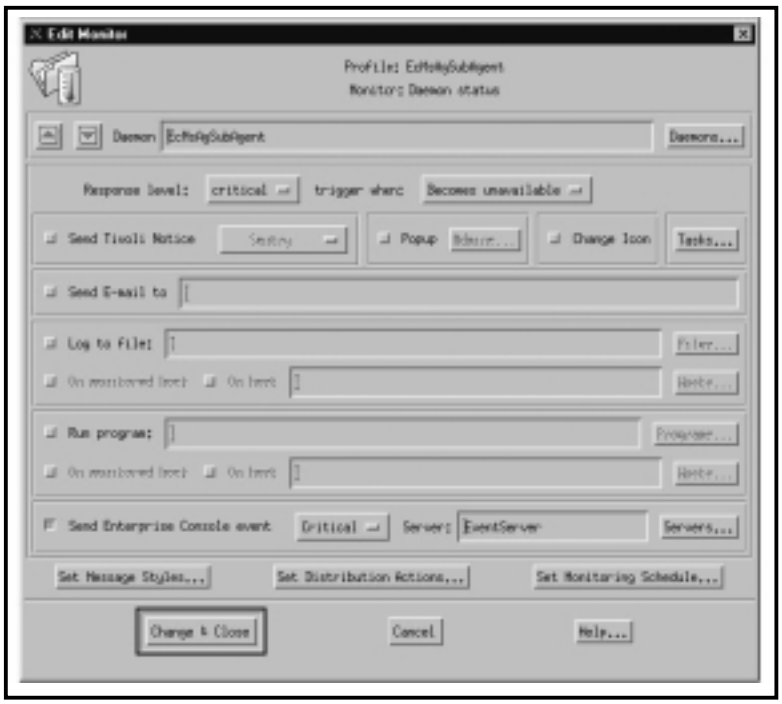

Figure 19. Daemon Monitor Profile Edit Page

Multiple monitoring profiles can be created and distributed across several hosts. Figure 20 shows a partial profile manager screen for performance monitors and their respective hosts.

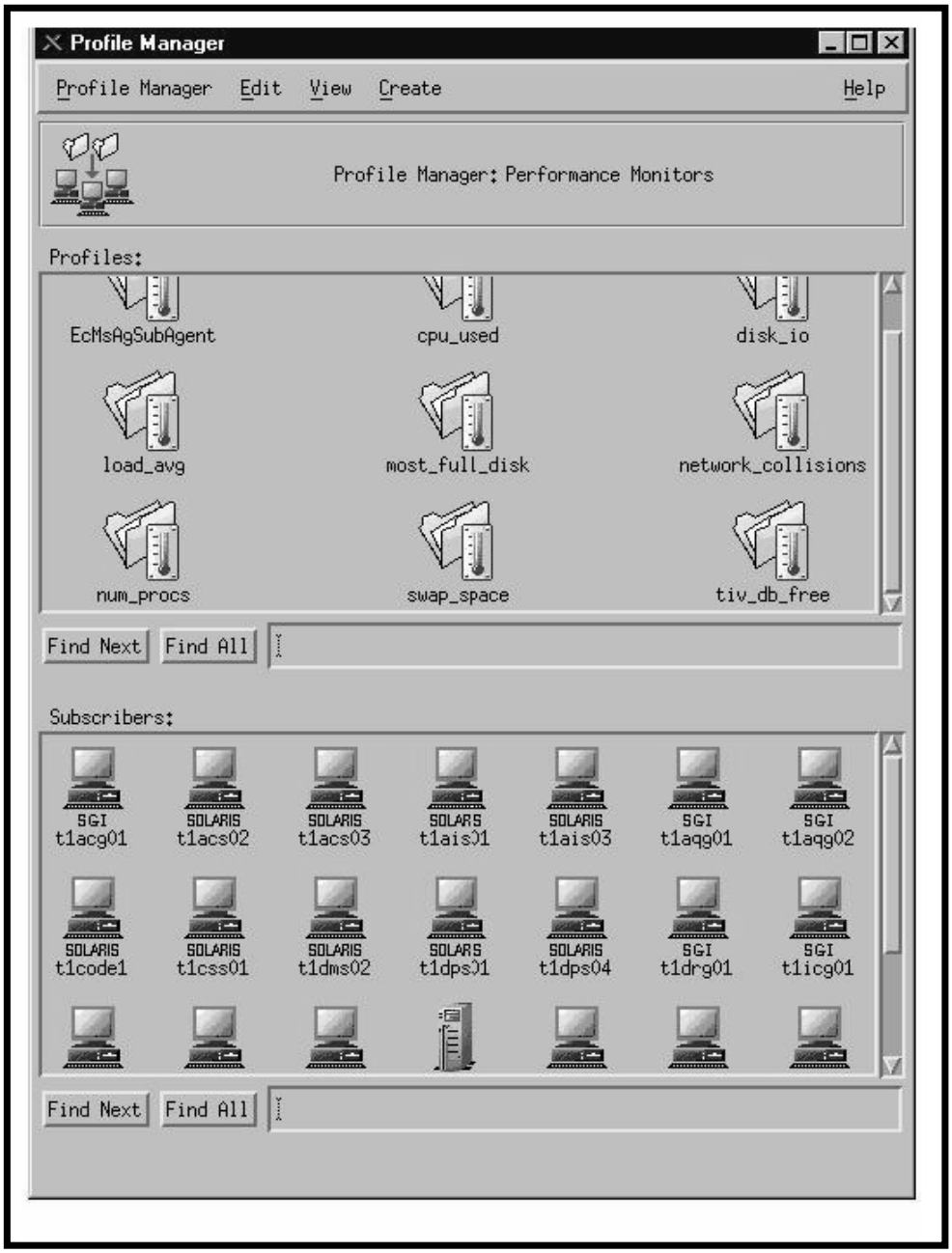

Figure 20. Performance Monitor Profile Manager screen

Administrators can also determine monitor profiles assigned to specific hosts. Figure 21 shows a portion of the monitor profiles active on host t1msh01 in the VATC.

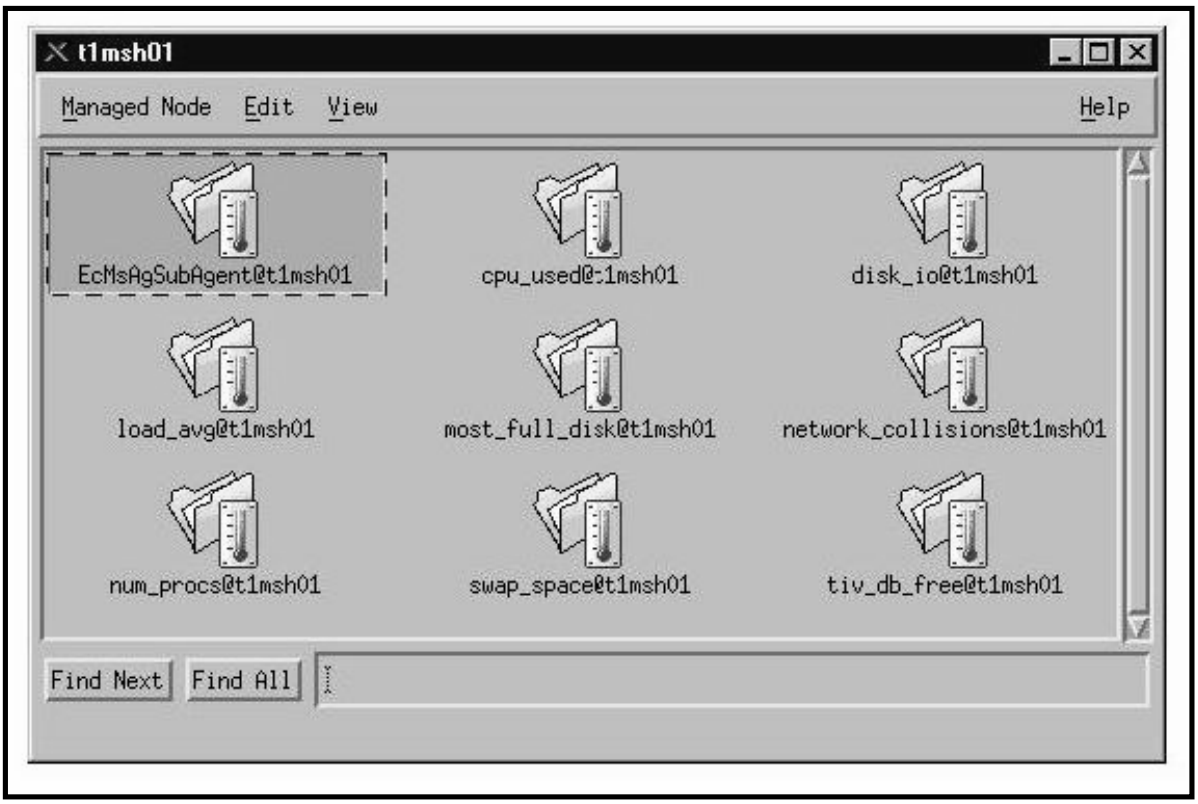

Figure 21. Monitor Profiles active for t1msh01

To determine Monitor Profiles active on a specific host, execute the procedure steps that follow:

Display Active Tivoli Monitor Profiles procedure

Start Tivoli using the Tivoli Startup Procedure.

- The Tivoli Startup screen appears temporarily, followed by the TME Administrator Desktop screen (Figure 17).

1 Double-click on the region icon to display Policy Region components.

- A scrollable window of components is displayed (Figure 18).

2 Double-click on any component icon.

- A scrollable window of Monitor Profiles is displayed (Figure 20).

3 Double-click on any specific Profile Monitor icon to determine profile characteristics (Figure 19).

Tivoli Enterprise Console

The component of Tivoli Management Environment that provides the interface for system monitoring is the Tivoli Enterprise Console. It monitors events defined by the administrator across individual or groups of items. An event is any significant change in the state of an application or system resource, such as a network or host. The Event Console is the interface

that an administrator uses to receive notification of events and to respond to events. An Event Group is depicted in the Event Groups event console dialog. There is one icon for each event group that is monitoredFigure 22 shows the Tivoli Enterprise Console Event Groups for the VATC.

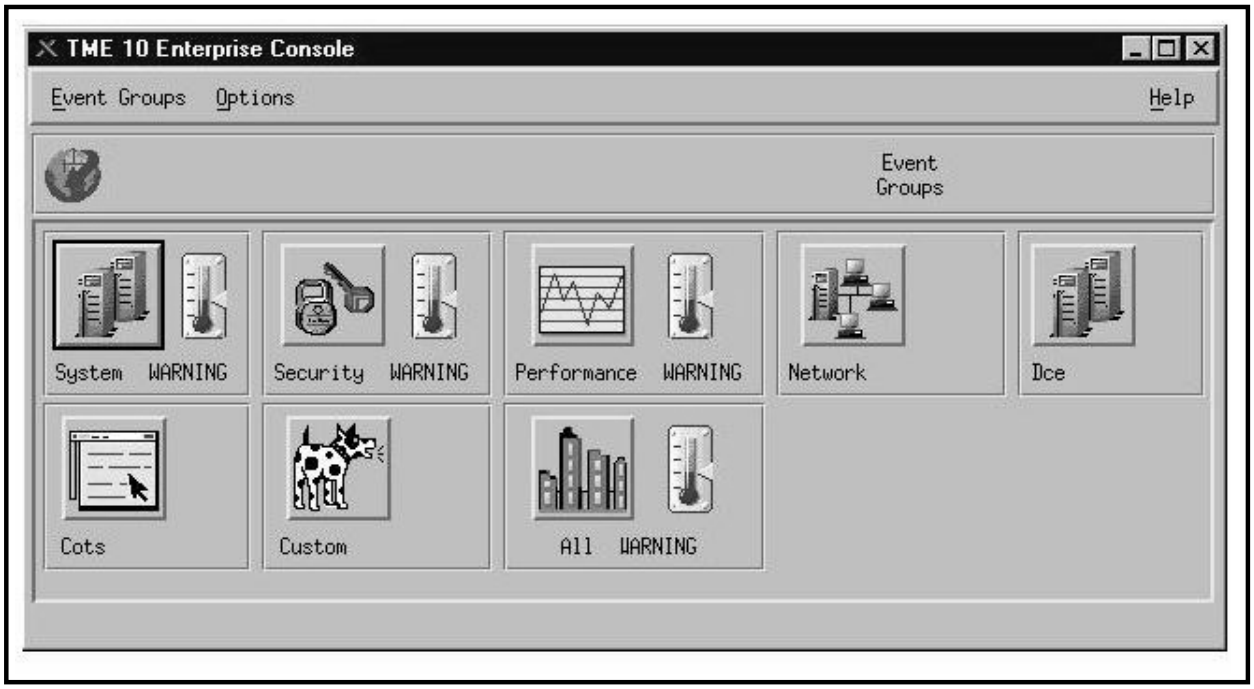

Figure 22. Tivoli Enterprise Console Event Groups

As in previous hierarchical displays, the Enterprise Console icons can be stepped through to determine specific errors in addition to any programmed notifications as determined by the administrator.

For detailed information and specific configuration and utilization of the Tivoli Management Environment, all documentation is available directly from the vendor in PDF format at the following URL: http://www.tivioli.com/support/documents.

.

Tape Operations

In this lesson you will learn how Networker Administrative software and the Exabyte tape drive work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

Terms:

- **Cartridge** - A hardware device that is part of the Exabyte tape drive. It holds up to 10 tapes that are automatically selected by Networker.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data.
- **Index** - A list of the labeled tapes currently stored in the jukebox.
- **Inventory** - The action of making an index.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task.
- **Label** - A unique name assigned to a tape by Networker.
- **Volume** - A recording medium; in the case of this course, a volume and a tape are synonymous.

Networker Administrator Screen

The main Networker Administrator screen (Figure 23), which is displayed after typing **nwadmin** at a UNIX prompt, contains four main sections:

1. The menu bar at the top of the screen, which displays all of the possible capabilities of Networker Admin.
2. The **speedbar**, which can be customized, displays icons that execute the most common procedures.
3. Current configuration information, including the current Networker server, the available backup devices (tape drives, file systems, CD-ROMs, etc.).
4. Current status windows which display in real time the actual activity on the various devices, and progress and error messages.

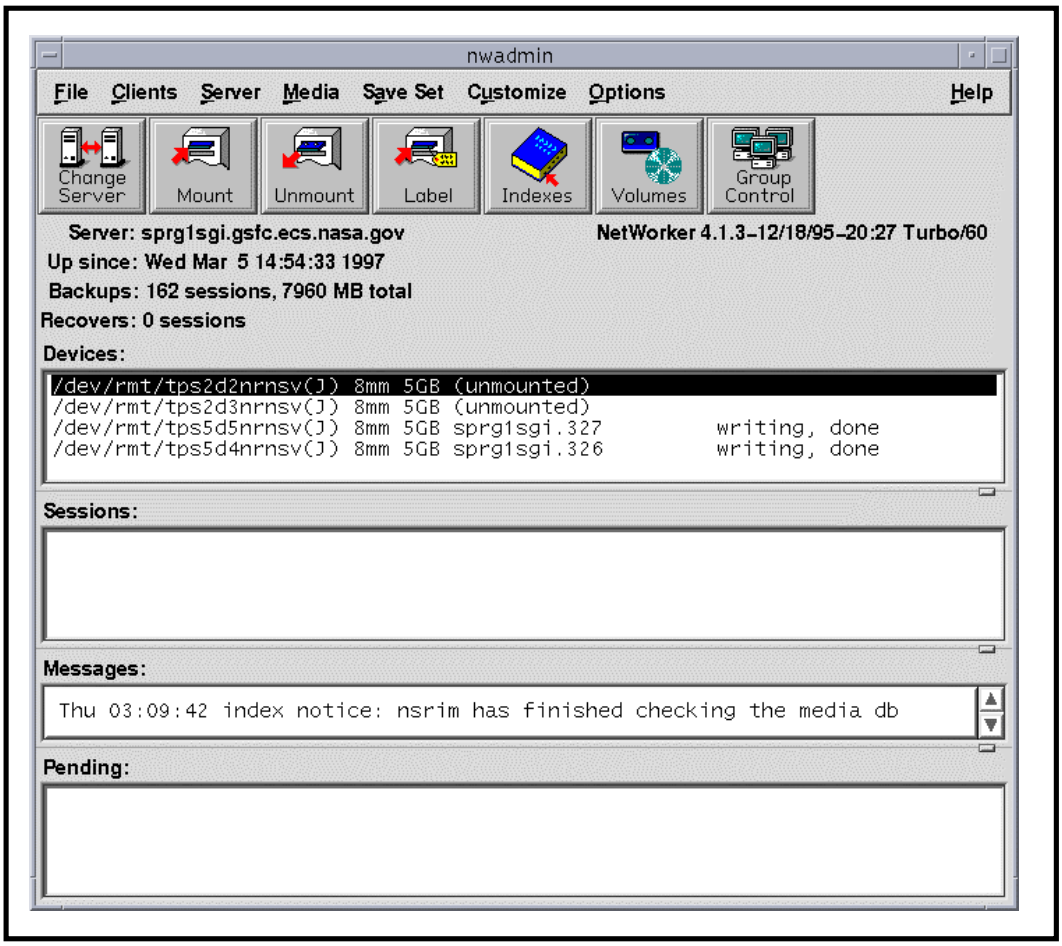

Figure 23. Networker Administrative main screen

Labeling Tapes

Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as Networker and such hardware devices such as the Exabyte jukebox to automate the tape selection process when performing system backups and restores. When a tape is initialized, Networker assigns it a label. Networker then stores the tape's label with a file that is written to the tape so that when a file restoration request is received, Networker will know exactly which tape to select from the jukebox.

Tape Labeling Procedure

1 Login to a system terminal.

2 Set display to current terminal by typing: **setenv DISPLAY <*IPNumber*>:0.0** then press **Return/Enter**

3 Start the log-in to the Backup client server by typing **/tools/bin/ssh *BackupServerName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing: **su**, then press **Return/Enter**.

- A password prompt is displayed.

7 Enter the ***RootPassword***, then press **Return/Enter.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

8 At the UNIX prompt, type **nwadmin**, then press **Return/Enter**.

- A window opens for the Networker Administrative program.

9 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

- Remove any non-blank tapes from the cartridge or else they will be re-labeled and the data on the tapes will be lost.

10 Click the **Label** button.

- The **Jukebox Labeling** window opens (Figure 24).

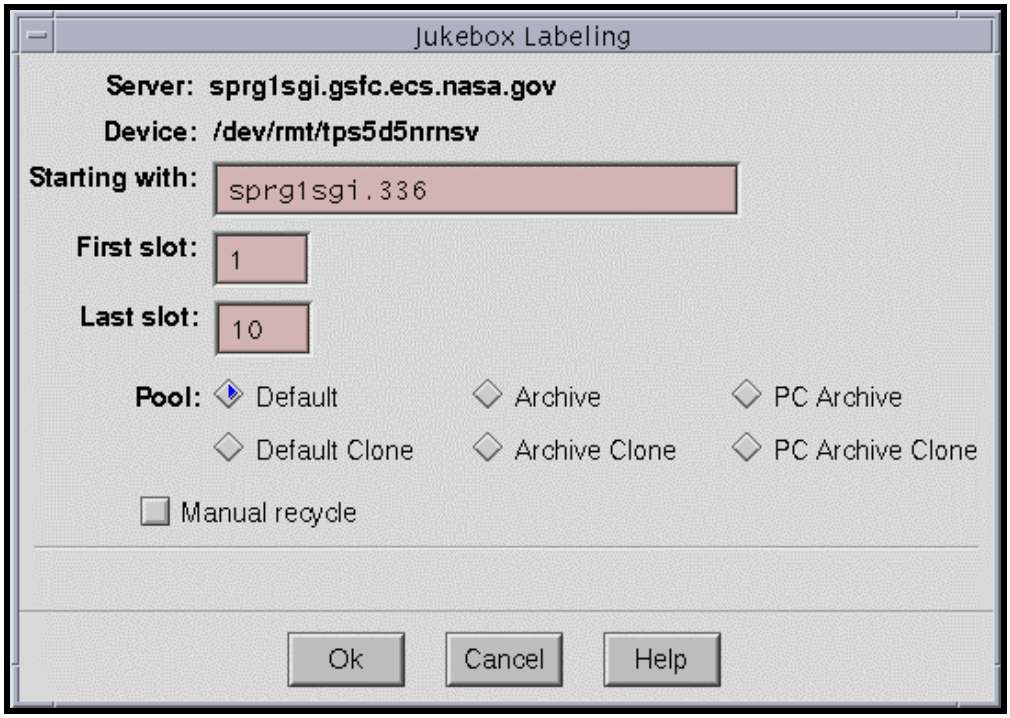

Figure 24. Jukebox Labeling window

11 In the field marked **Starting with**, enter the tape label you wish to use for the first tape in the sequence.

- Tape labels are named by using the host name (e.g., **sprn1sgi**), a dot or period, and a sequential number (e.g., **001**, **002**).
- By default, the system will prompt you with the next label in the sequence (e.g., **sprn1sgi.011**).

12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.

- Slot 1 is at the top of the cartridge and 10 at the bottom.
- Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
- It is OK to leave empty slots.

13 Click the **OK** button.

- A status message indicating the progress of the tape labeling procedure appears and updates.
- Labeling a full cartridge of tapes takes about 15 minutes.

14 When the status in the **Jukebox Labeling** window reads **finished**, click the **Cancel** button.

- The **Jukebox Labeling** window closes.

15 From the **File** menu, select **Exit**.

- The **nwadmin** program terminates and you are returned to the UNIX prompt.

16 At the UNIX prompt for the backup server, type **exit**, then press **Return/Enter**.

- **Root** is logged out.

17 Type **exit** again, then press **Return/Enter**.

- You are logged out of and disconnected from the backup server.

18 Put an identifying sticker on the outside of each tape cassette.

Indexing Tapes

Labeled tapes are loaded in a tape cartridge that is inserted into the Exabyte tape drive, also referred to as the *jukebox.* Networker needs to know the location of each tape in the jukebox. To do this, Networker uses a process called **inventory** which prepares an index by matching a tape label to the cartridge slot that holds that tape (Figure 25). Then, when a request to recover a file or a set of files is received, *Networker* locates the tape based on the information in its memory.

CAUTION

*If you move a tape from its position in the cartridge, Networker will not know where to find it (***Figure 26***). You must re-index the cartridge by performing these procedures again for Networker to select the correct tape (***Figure 27***).*

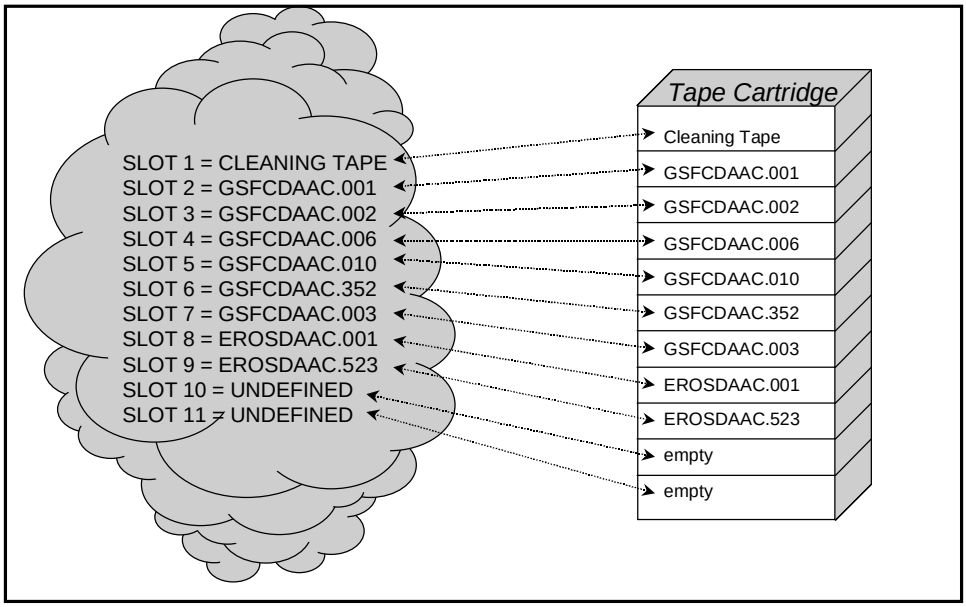

Figure 25. Tape index following the initial inventory.

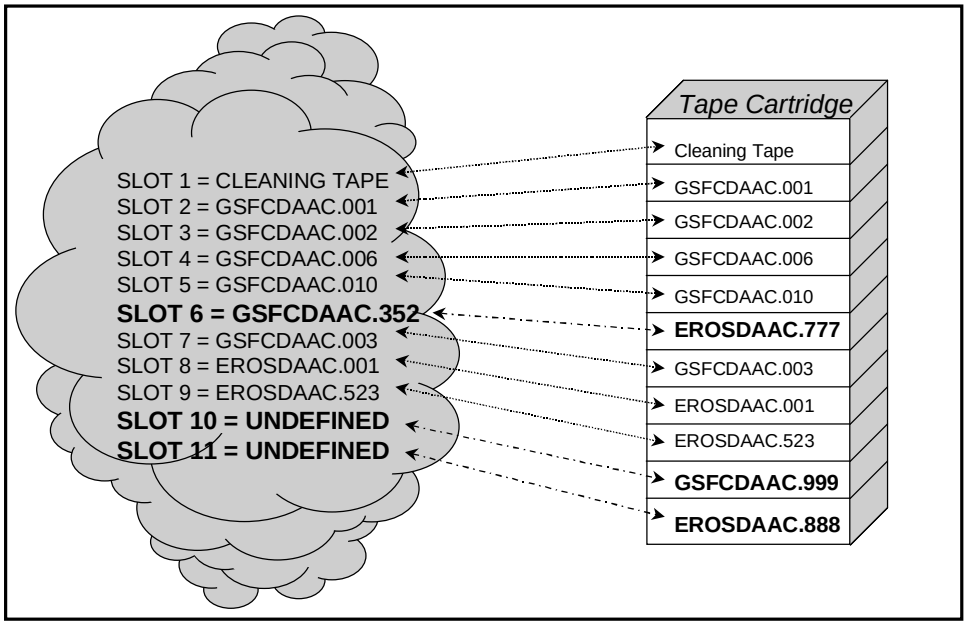

Figure 26. Tapes changed but not re-inventoried.

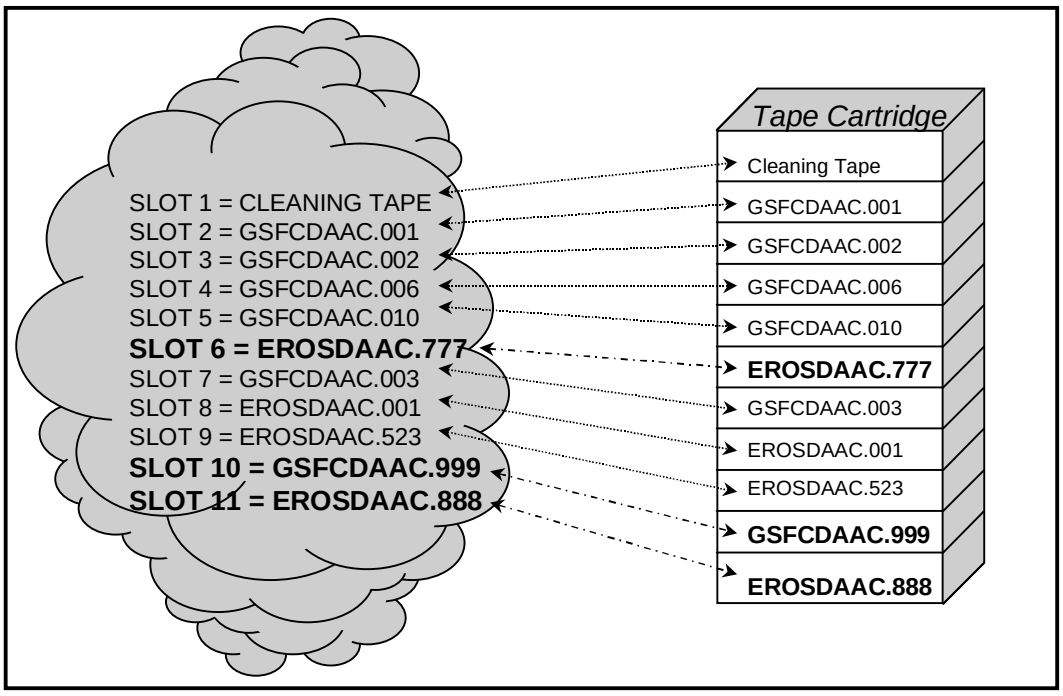

Figure 27. Index is updated after re-inventory.

Indexing Tape Procedure

1 Login to a system terminal.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** , then press **Return/Enter**.

3 Start the log-in to the Backup client server by typing **tools/bin/ssh *BackupServerName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

8 At the UNIX prompt, type **nwadmin**, then press **Return/Enter**.

- A window opens for the **Networker Administrative** program.

9 Click the **Mount** button, or select **Media -> Mount** from the menu.

- The **Jukebox Mounting** window opens (Figure 28) and displays a list of the tapes that Networker is currently aware of.
- When you are finished with this window, click the **Cancel** button.

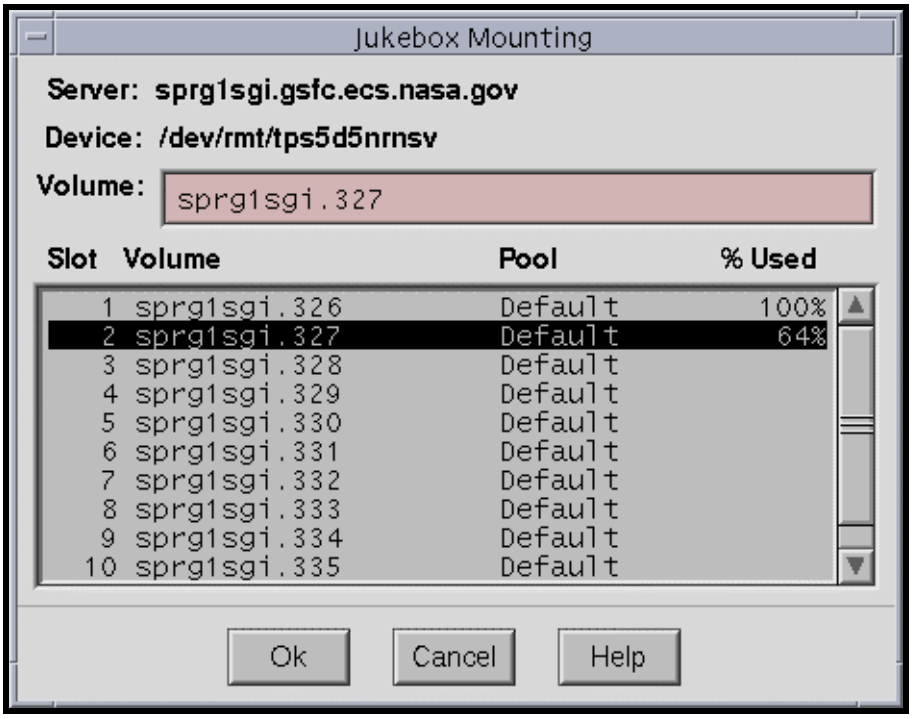

Figure 28. Jukebox Mounting window.

10 Insert the required tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

- Refer to the jukebox's documentation for detailed instructions on installing the cartridge.

11 Select **Media** from the menu bar, then select **Inventory**.

- The **Jukebox Inventory** window opens.

12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.

- Slot 1 is at the top of the cartridge and 10 at the bottom.
- Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
- It is OK to leave empty slots or slots with previously inventoried tapes.

13 Click the **OK** button.

- A status message indicating the progress of the tape indexing procedure appears and updates.
- Inventorying a full cartridge of tapes takes between 20 and 30 minutes.

14 When the **Jukebox Inventory** status reads **finished**, click the **Cancel** button.

15 Click the **Mount** button to verify that the indexing worked.

- The **Jukebox Mounting** window opens.
- The **required tape(s)** should be shown. If not, repeat this procedure from step 9.

16 Click the **Cancel** button.

- The **Jukebox Mounting** window closes.

17 From the menu bar, select **File**, then select **Exit**.

18 At the UNIX prompt for the ***BackupServer***, type **exit**, then press **Return/Enter**.

19 At the next UNIX prompt, type **exit** again, then press **Return/Enter**.

This page intentionally left blank.

System Backups and Restores

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator has. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore the data from the backup tapes depending on backup method(e.g., full or partial).

Incremental Backup

An incremental backup copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users. Copies of all incremental backup tapes are stored offsite for five weeks before they are reused.

Incremental backups are performed automatically according to the schedule setup in the Networker.

Schedules windows (Figure 29). Incremental backups can also be requested at unscheduled times by completing the **Incremental Backup Request Form** and submitting it to the DAAC manager.

On-Demand Incremental Backup Procedure

1 Login to a system terminal.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0**, then press **Return/Enter**.

3 Start the log-in to the Backup client server by typing **tools/bin/ssh *BackedUpSystemName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

7 A password prompt is displayed.

8 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

9 At the UNIX prompt, type **nwadmin**, then press **Return/Enter**.

- A window opens for the Networker Administrative program.

10 Go to the **Customize** menu, select **Schedules**.

- The **Schedule**s window opens.

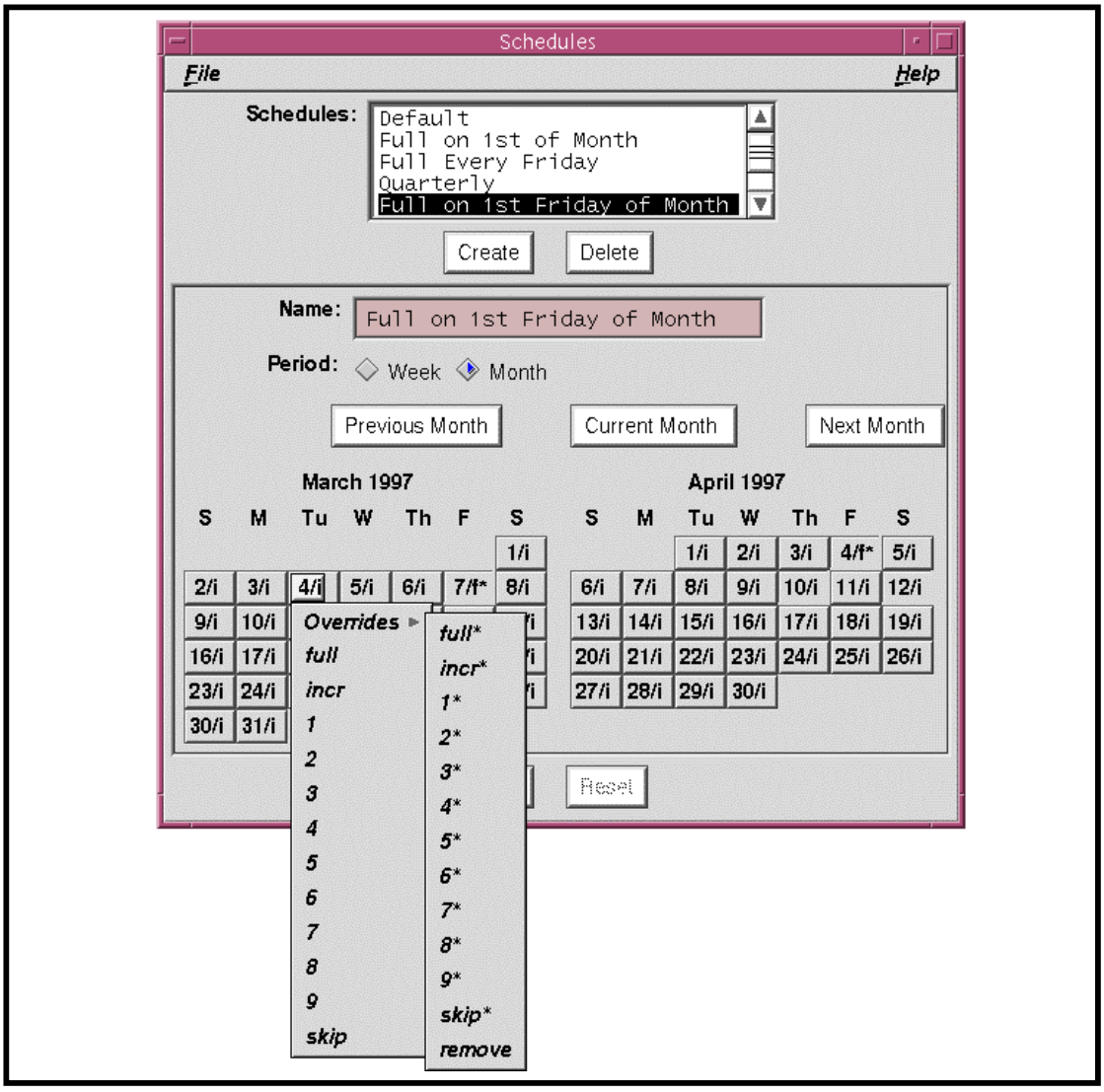

Figure 29. Networker Schedules window.

11 Look at the button for today and note the letter on that day. If there is an **i** next to the date on this button, go to step 12.

- The **i** stands for incremental; **f** stands for full. Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.

12 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.

13 Click the **Apply** button.

14 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

15 Click the **Group Control** button.

- The **Group Control** window opens.

16 Click the **Start** button.

- A **Notice** window opens.

17 Click the **OK** button.

- The **Notice** window closes.
- The regularly scheduled backup will still run (even though we are now doing a backup).

18 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.

- Status updates appear in the **nwadmin** window.
- When the backup is complete, a **Finished** message will appear.

19 If the button for today in step 11 had an i on it, go to step 23.

20 Go to the **Customize** menu, select **Schedules**.

- The Schedules window opens.

21 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.

22 Click the **Apply** button.

23 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

24 Select **Exit** from the **File** menu to quit the NetWorker Administrative program.

- The **nwadmin** window closes.

25 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return/Enter**.

- Root is logged out.

26 Type **exit** again, then press **Return/Enter**.

- You are logged out and disconnected from the machine to be backed up.

Full System Backup

A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a total system failure. The full system backup is run by the System Administrator on a regular schedule, usually weekly. Full system backup tapes are stored offsite for security reasons.

Full Backup Procedure

1 Login to a system terminal.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0**, then press **Return/Enter**.

3 Log into the machine to be backed up by typing: **/tools/bin/ssh *BackedUpSystemName***, then press **Return/Enter**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

8 Execute the NetWorker Backup program by entering: **nwbackup**, then press **Return/Enter**.

- A **NetWorker Backup** window opens (Figure 30). You are now able to perform a full backup.

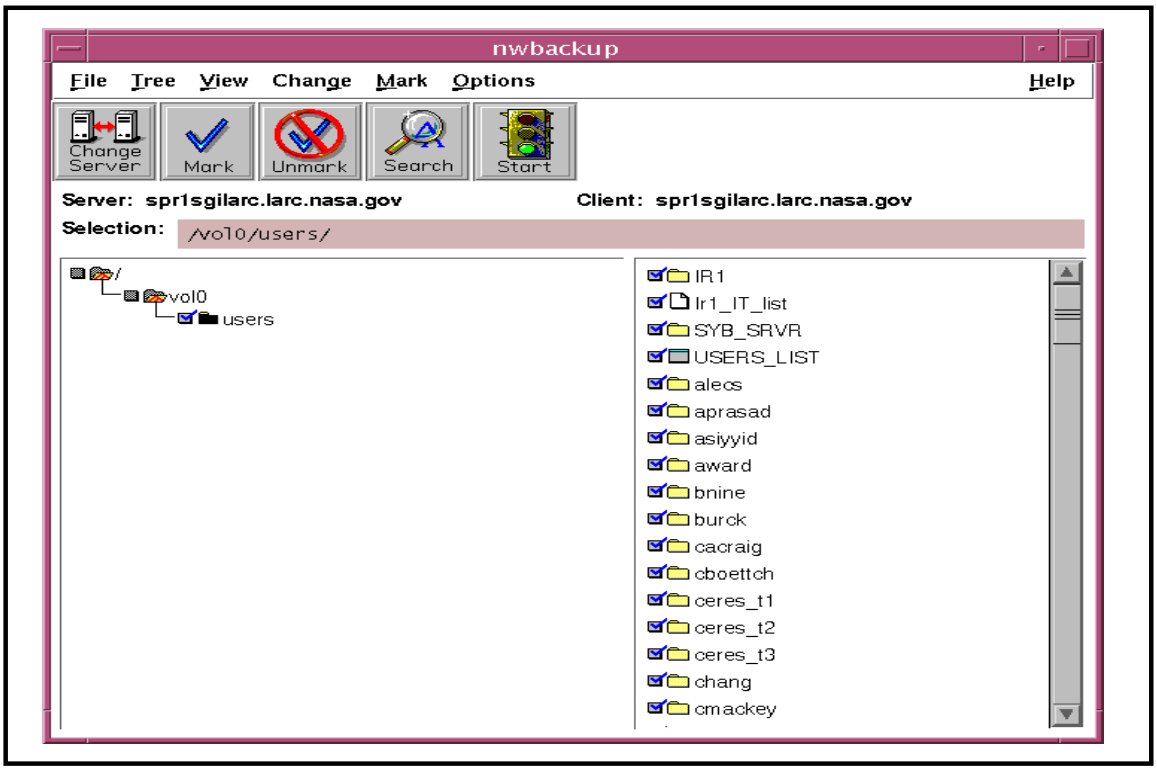

Figure 30. Networker Backup Window.

9 If no **files/directories to be backed** up were provided by the requester, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.

- **/** is designated for backup and has a check next to it.

10 If **files/directories to be backed up** were provided, then select the **files/directories to be backed up** in the directory display and click the **Mark** button.

- Drag scroll bar with the mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.
- Clicking the **Mark** button designates the file for backup and puts a check next to it.

11 Click the **Start** button.

- A **Backup Options** window opens.

12 Click the **OK** button.

- The **Backup Options** window closes.
- The **Backup Status** window opens providing updates on the backup's progress.

13 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.

- The **Backup Status** window closes.
- The backup is complete.

14 Select **Exit** from the **File** menu to quit the NetWorker Backup program.

- The NetWorker Backup window closes.

15 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return/Enter**.

- Root is logged out.

16 Type **exit** again, then press **Return/Enter**.

- You are logged out and disconnected from the machine to be backed up.

Single or Multiple File Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.
- User ID of the owner of the file(s) to be restored.
- Choice of action to take when conflicts occur. Choices are:
  - ❏ rename current file.
  - ❏ keep current file.
  - ❏ write over current file with recovered file.

Single or Multiple File Restore Procedure

1 Login to a system terminal.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0**, then press **Return/Enter**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return/Enter**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

8 Log in as the user by typing: **su *User'sID.***

- You are authenticated as the owner of the file(s) to be restored.

9 Execute the NetWorker Recovery program by entering: **nwrecover**, then press **Return/Enter**.

- A window opens for the **Networker Recovery** program (Figure 31). You are now able to restore files.

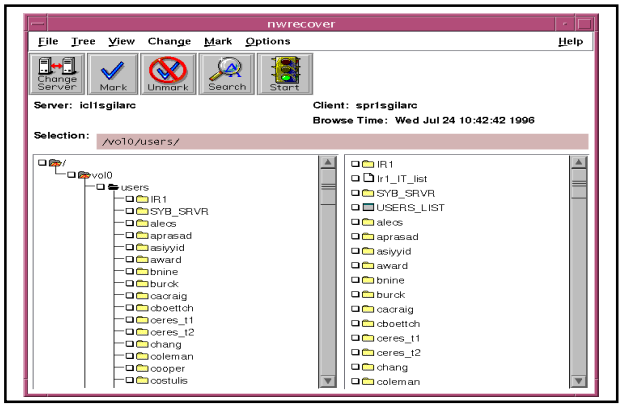

Figure 31. Networker Recovery Window.

11 Select **file(s) to be restored** and click the **Mark** button.

- Drag scroll bar with the mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- Clicking the **Mark** button designates the file for restore and puts a check next to it.

12 Go to the **Change** menu, select **Browse Time**.

- The **Change Browse Time** window opens.

13 Select the **date from which to restore**.

- Networker will automatically go to that day's or a previous day's backup which contains the file.

14 Click the **Start** button.

- The **Conflict Resolution** window opens.

15 Answer "Do you want to be consulted for conflicts" by clicking the **yes** button, then click the **OK** button.

- If prompted with a conflict, choices of action will be: rename current file, keep current file, or write over current file with recovered file.
- Select the requester's **choice of action to take when conflicts occur.**
- The **Recover Status** window opens providing information about the to be restored.
- If all the required tapes are not in the drive, a notice will appear.
- Click the **OK** button in the notice window.

16 When a **recovery complete** message appears, click the **Cancel** button.

17 Go to the **File** menu, select **Exit**.

- The Networker Recovery program quits.

18 Type **exit**, then press **Return/Enter**.

- The owner of the file(s) to be restored is logged out.

19 Type **exit** again, then press **Return/Enter**.

- Root is logged out

20 Type **exit** one last time, then press **Return/Enter**.

- You are logged out and disconnected from the **machine to be restored**.

Complete System Restore

A complete system restore is an emergency procedure that should be performed only in the event of a system crash with the loss of data. The only way to get the system back up and running in a timely fashion is to restore the system from a previous backup. The result of this action will be that any updates to the system between the last backup and the time of the restore will be lost. The System Administrator will determine which complete backup tape(s) to use (Figure 32). Depending on the frequency of complete system backups and incremental backups, data loss can be minimized.

A complete system restore involves restoring a number of tapes depending upon the particular situation. For example, should a system failure occur immediately after a full system backup was performed, only the tapes used in that backup will be required to restore the system to its usable state. However, if there was a period of time between the last full system backup and the system failure, tapes from the last full system backup as well as partial and incremental backups will have to be restored. This may become a time consuming process depending on the server affected, how much data is to be recovered, and how many tapes need to be restored. Additionally, the System Administrator may determine that only one or two of the many partitions need to be restored to make the system whole again. Therefore, these procedures will have to be mixed and matched to determine the proper restoration procedure for a given situation.

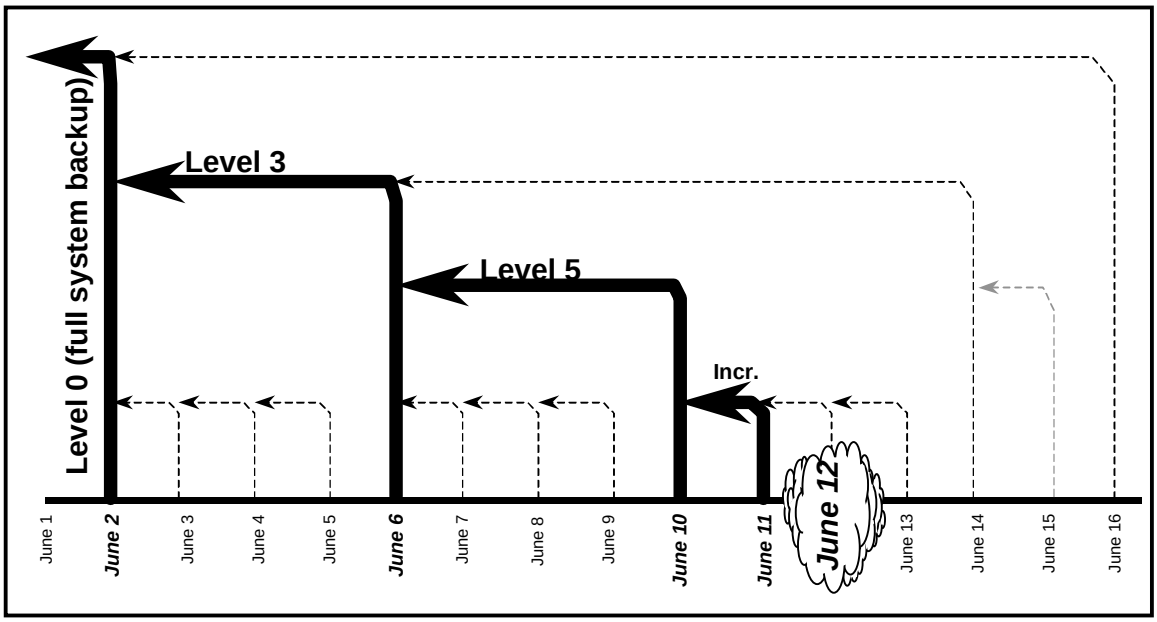

Figure 32. Tapes Required for Full System Restore.

In order to perform the procedure, the SA must have obtained the following information about the requester:

- Name of system to be restored
- Date from which to restore

Full System Restore Procedure

---

1 Log into the backup server by typing: **/tools/bin/ssh *BackupServerName***, then press **Return/Enter**.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0**, then press **Return/Enter**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return/Enter**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

8 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return/Enter**.

9 Log in as the user by typing: **su *User'sID.***

- You are authenticated as the owner of the file(s) to be restored.

10 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *MachineRestored*:0.0**, then press **Return/Enter**.

11 Execute the Networker Administrator program by entering: **nwadmin**, then press **Return/Enter**.

- A window opens for the Networker Administrator program (Figure 33).
- You are now able to perform restores of partitions.

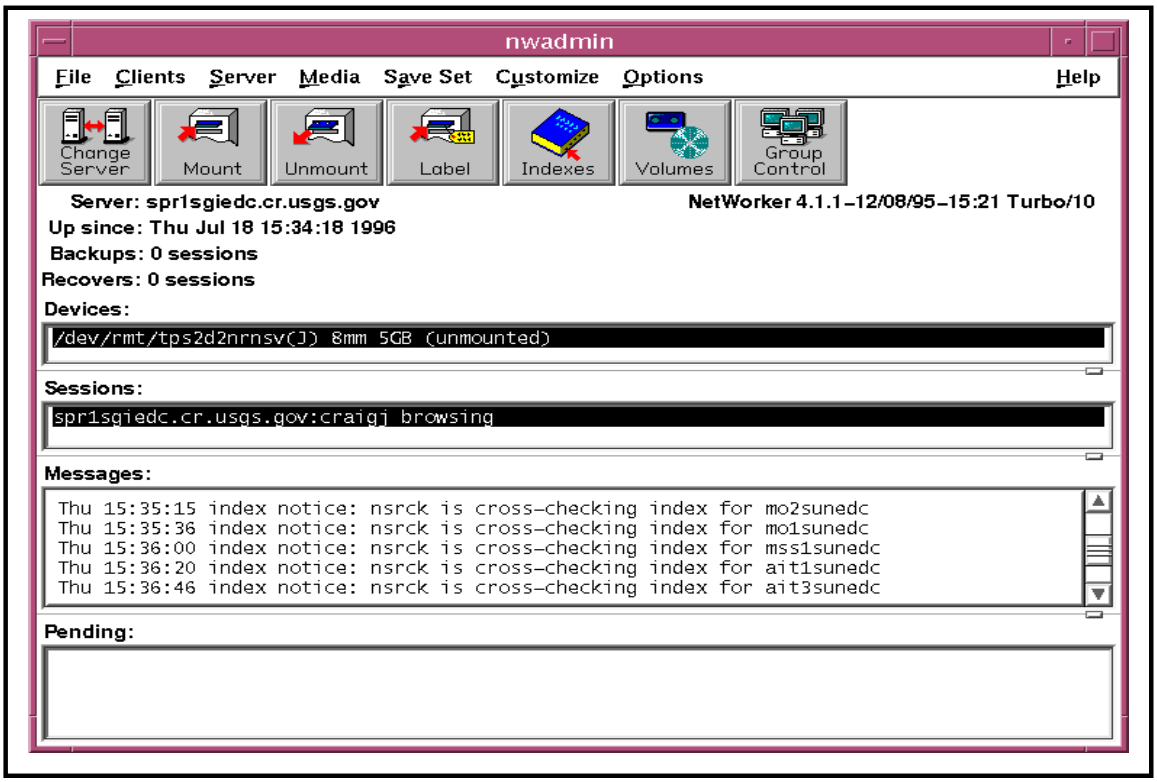

Figure 33. Networker Administrator's Window.

12 Go to the **Save Set** menu, select **Recover Set.** The **Save Set Recover** window opens.

13 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.

- The **Save Set** listing updates. This is a listing of partitions on the **System**.
- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.

14 Select the **Save Set**/partition from the listing.

- The **Instance** listing updates.

15 Select the appropriate **Instance**.

- An **Instance** is a particular NetWorker client backup. A listing of **Instances** is a report detailing the Networker client backups that have occurred.
- Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:

Note: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.

- If the backups are full or incremental, perform the following actions:

Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.

- If the backups are of different numerical levels, follow these steps:

First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**. Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

16 Click the **Recover** button.

- The Save Set Recover Status window opens.
- Clicking the Volumes button will show which tapes are required.

17 Click the **Options** button.

- The Save Set Recover Options window opens.

18 Set Duplicate file resolution to Overwrite the existing file by clicking its radio button.

19 Make sure that the **Always prompt** checkbox is not checked.

20 Click the **OK** button.

- The **Save Set Recover Options** window closes.

21 Click the **Start** button in the **Save Set Recover Status** window.

- Status messages appear in the **Status** box.
- A **recovery complete** message appears when recovery is complete.

22 Click the **Cancel** button after the **recovery complete** message appears.

- The **Save Set Recover Status** window closes.

23 If additional partition restores are required, go to step 12. Otherwise, select **Exit** from the **File** menu to quit the Networker Administrator program.

24 At the UNIX prompt for the backup server, type **exit**, then press **Return/Enter**.

25 Type **exit** again, then press **Return/Enter**.

System Log Maintenance

System Log Maintenance

The System Log Maintenance process is performed through Tivoli by the System Administrator. The System Administrator will setup and execute the jobs to be run in various formats, e.g., recurring day and time, maximum amount of disk space. This section assumes that task jobs have already been created and discusses how to edit the job for System Log Maintenance.

Logs are used to track events on the system. An *event* is the success or failure of an action. By reading and maintaining logs, System Administrators can troubleshoot problems. Entries to the logs are automatically created by the particular application and stored in the directory /usr/local/hislog in a file with a *.log* suffix (e.g., IngestLocal.log).

System Log Maintenance Procedure

1 Log in to a **Tivoli server** by typing: **/tools/bin/ssh *TivoliServerName*** at the UNIX prompt, then press **Return/Enter**.

2 Set display to the current terminal by typing: **setenv DISPLAY *IPNumber*:0.0**, then press **Return/Enter**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return/Enter**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return/Enter.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return/Enter**.

- You are authenticated as root and returned to the UNIX prompt.

8 Enter **tivoli**, then press **Return/Enter**.

- The **TME Desktop Administrator** window (Figure 34) appears.

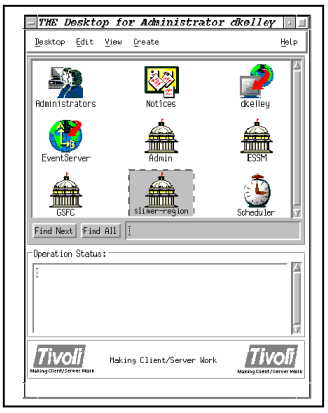

Figure 34. TME Administrator Window.

9 Double-click on the **Scheduler** icon (Figure 35).

Figure 35. Scheduler icon.

10 Click once on the job you wish to edit so that it is highlighted.

11 Select **Edit** from the menu at the bottom of the screen.

- You will now be in the **Edit Scheduled Job** window.

12 Make all of the desired changes.

13 After changes have been made, select **Update & Close** from the menu at the bottom of the window.

- Type **exit**, then press **Return/Enter**.
- You are logged out of the Tivoli server.

User Administration

Adding a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line, or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The scripts will accomplish these steps in an interactive manner.

The requester fills out a "User Registration Request Form" and submits it to the requestor's supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority; the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd.yp** (Figure 36), **/etc/group** (Figure 37), and **/etc/auto.home** .

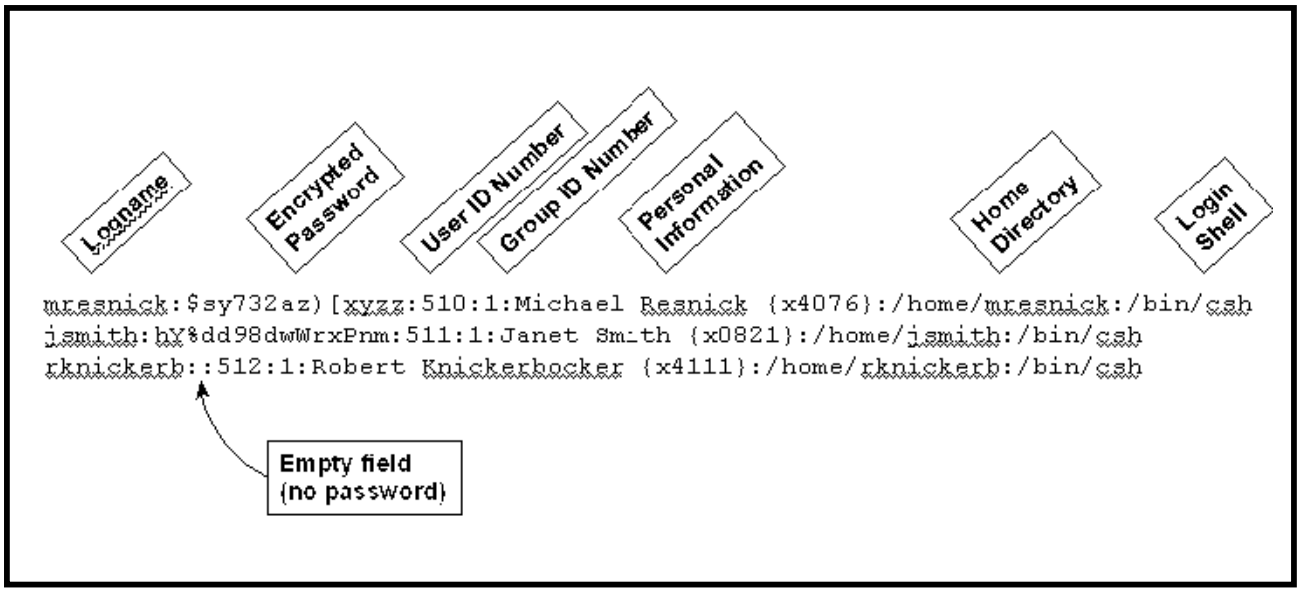

Figure 36. /etc/passwd.yp File Fields.

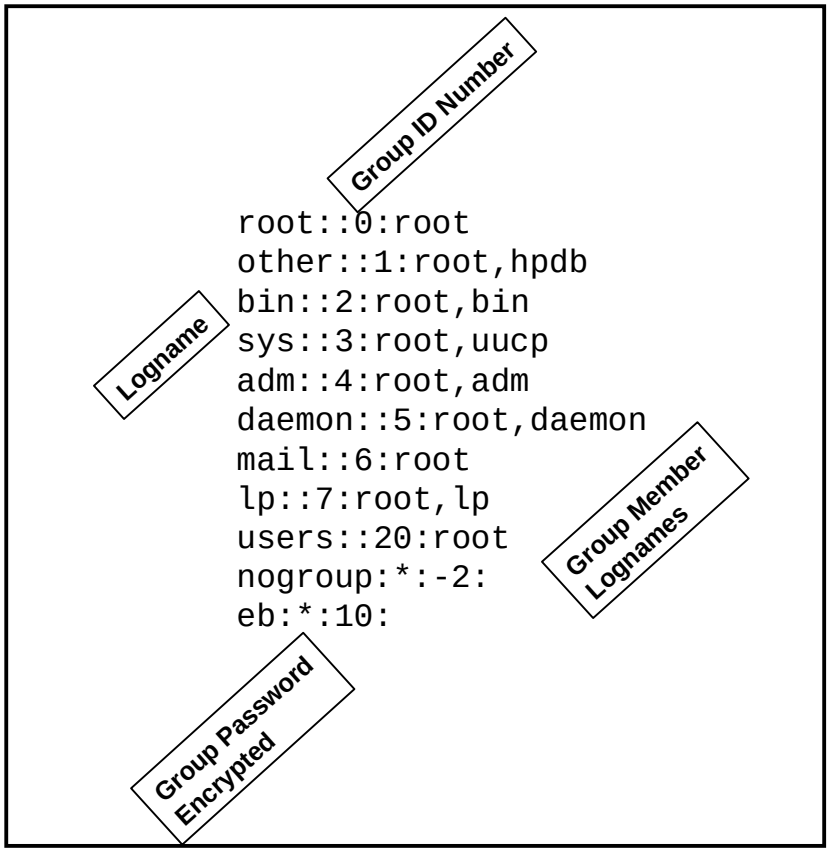

Figure 37. /etc/group File.

The System Administrator (SA) creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **UNIX login of the user to be deleted**

b. **Role(s) of the user to be deleted**

The System Administrator deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion, deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

Changing a User's Account Configuration

Account configuration is accomplished through command line and script. The DAAC manager must authorize changes to user accounts.

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Super detailing what to change about the account configuration and the reason for the change. The OPS Super reviews the request and forwards it to the SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Super.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- What to change and new settings. Can be any of:
  - ❏ New Real User Name
  - ❏ New Office Number
  - ❏ New Office Phone Number
  - ❏ New Home Phone Number
  - ❏ New UNIX Group
  - ❏ New DCE Group
  - ❏ New DEC Organization
  - ❏ New Login Shell
- Current UNIX Login of the User

Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the Ops Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Role(s) to which the user is to be added
- Role(s) from which the user is to be removed
- UNIX login of the user

Changing a User Password

The Changing a Users Password process begins when the requester submits a request to the SA. The System Administrator verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New password for the user**

To change a user password for the requester, execute the command line or script procedure steps that have been developed.

Checking a File/Directory Access Privilege Status

Checking File/Directory Access Privileges Procedure

1 At a UNIX prompt, type **cd *Path***, press **Return/Enter.**

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe, then type **cd /home** and press **Return/Enter**.

2 From the UNIX prompt, type **ls -la**. The output from the command should appear as below:

```
drwxrwxrwx    3    mresnick    training    8192    Jun 14 08:34    archive
drwxr-xr-x   11    mresnick    training    4096    Jul 03 12:42    daacdata
-rw-rw-rw-    1    mresnick    training     251    Jan 02 1996     garbage
lrw-r--r--    2    jjones      admin      15237    Apr 30 20:07    junk
-rwxr--rw-    1    mresnick    training    5103    Oct 22 1994     trash
```

- The first column of output is the file access permission level for the file (see Figure 48 below for a description of file permissions).
- The next column to the right is the number of links to other files or directories.
- The third column is the file owner's user ID
- The fourth column is the group membership of that owner.
- The fifth column shows file size in bytes.

- The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)
- The last column displays the file name.

Changing a File/Directory Access Privilege

File and directory access privileges are displayed in the first output column of the **ls -l** command and consists of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 38:

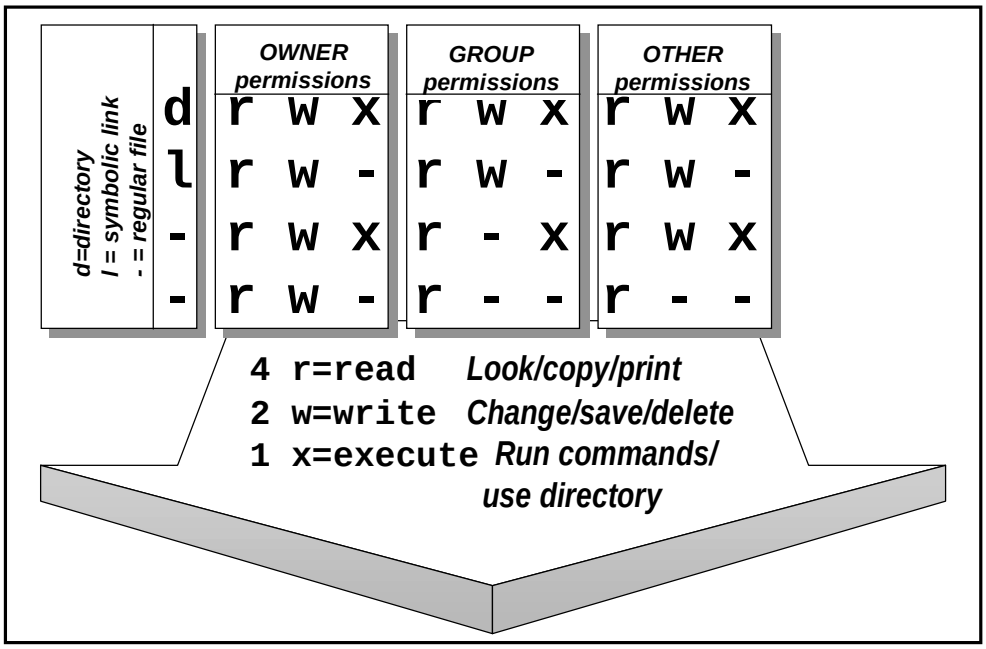

Figure 38. Access permissions.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- full path of the file/directory on which access privileges will be changed.
- new access privileges to set on the file/directory. Can be any of:
  - ❑ New owner
  - ❑ New group
  - ❑ New user/owner privileges (read, write and/or execute)
  - ❑ New group privileges (read, write and/or execute)
  - ❑ New other privileges (read, write and/or execute)

Changing a File/Directory Access Privilege Procedure

1 At the UNIX prompt, type **su**, press **Return/Enter**.

2 At the **Password** prompt, type ***RootPassword***, press **Return/Enter**.

- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **cd *Path***, press **Return/Enter**.

- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return/Enter**.

4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName***, press **Return/Enter**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chown *NewOwner* jdoe** and press **Return/Enter**.

5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName***, press **Return/Enter**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chgrp *NewGroup* jdoe** and press **Return/Enter**.

6 If there are **New user/owner privileges** then type **chmod u=*NewUserPrivileges FileOrDirectoryName***, press **Return/Enter**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod u=*NewUserPrivileges* jdoe**, press **Return/Enter**.
- The ***NewUserPrivileges*** are r for read, w for write and x for execute. For example, to give the user/owner read, write and execute privileges, type **chmod u=rwx *FileOrDirectoryName*** and press **Return/Enter**.

7 If there are **New group privileges** then type **chmod g=*NewGroupPrivileges FileOrDirectoryName***, press **Return/Enter**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod g=*NewGroupPrivileges* jdoe**, press **Return/Enter**.

- The ***NewGroupPrivileges*** are r for read, w for write and x for execute. For example, to give the group read and execute privileges, type **chmod g=rx *FileOrDirectoryName*** and press **Return/Enter**.

8 If there are **New other privileges** then type **chmod o=*NewOtherPrivileges* *FileOrDirectoryName***, press **Return/Enter**

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod o=*NewOtherPrivileges* jdoe**, press **Return/Enter**.
- The ***NewOtherPrivileges*** are r for read, w for write and x for execute. For example, to give others read privileges, type **chmod o=r *FileOrDirectoryName*** and press **Return/Enter**.

9 Type **exit**, press **Return/Enter**.

- Root is logged out.

Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

This page intentionally left blank.

Commercial Off-the-Shelf (COTS) Administration

What is COTS?

The ECS organization provides maintenance and operations for ECS hardware, software, and firmware systems delivered under the ECS contract at the ECS sites. Commercial off-the-shelf software, firmware, and hardware will be maintained in accordance with the COTS Maintenance Plan, CDRL 613-CD-001-001. The project maintenance philosophy for software is to provide ECS centralized support for developed items and vendor-directed support for COTS software.

Installation

ECS Project software consists of COTS, custom, and science software.

Software maintenance includes:

- • A COTS support contract with the software vendor for license to use, telephone assistance in resolving COTS software problems, obtaining patches and obtaining upgrades.
- • Resources, including equipment, software tools and personnel to maintain ECS in accordance with specified functional, performance, and availability requirements.
- • Services required to produce, deliver, integrate, install, test, validate and document corrections and modifications of existing ECS software and firmware. The maintenance activity includes: software configuration management (CM) including support for change control, configuration status accounting, audit activities, and software quality assurance (QA). Each site is the CM authority over its own resources subject to ESDIS delegation of roles for ECS management.

Log files

Log files shall be maintained documenting all COTS installations and modifications. These files delineate manufacturer, product, installation date, modification date and all other pertinent configuration data available.

COTS configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. The ECS Sustaining Engineering Office (SEO) notifies the CCB of the upgrade that has been received. The ECS Property Administrator distributes the COTS software upgrade as directed by the CCB. The site Software Maintenance Engineer, Network Administrator, and the

System Administrator are responsible for upgrading the software on the host machine and providing follow-up information to the Configuration Management Administrator (CMA) and the ECS Property Administrator. The site Local Maintenance Coordinator will notify the appropriate personnel (Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer) when the COTS software is received and approved by the CCB for installation.

COTS software patches may be provided by the COTS software vendor in response to a DAAC's call requesting assistance in resolving a COTS software problem. The problem may or may not exist at other locations. When a COTS software patch is received directly from a COTS software vendor (this includes downloading the patch from an on-line source), the DAAC's CCB will be informed via CCR prepared by the requesting Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer. It is the responsibility of the Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer to notify the CCB of the patch's receipt, purpose, and installation status and to comply with the CCB decisions. The Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer installs COTS software patches as directed by the CCB.

In addition to providing patches to resolve problems at a particular site, the software vendor will periodically provide changes to COTS software to improve the product; these changes are issued as part of the software maintenance contract. Upgrades are issued to licensees of the basic software package. Therefore, the COTS software upgrades will be shipped to the ECS Property Administrator, who receives and enters them into inventory.

Security

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. To monitor and control access to network services, ECS Security Services uses the public domain tool, TCP Wrappers. Three other public domain COTS products — npassword, Crack, and SATAN — provide additional password protection for local system and network access. The tool, Tripwire, monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for M&O personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

Generating Security Reports

Reviewing User Activity Data

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file **/var/adm/loginlog**. The procedures assume that the file has been created and the operator has logged on as root.

Reviewing User Activity Data Procedure

1 At the UNIX prompt, type **/usr/bin/logins [-admopstux] [-g group..] [-l login..],** then press **Return/Enter**.

2 Type **logins -x -l *username,*** then press **Return/Enter**.

- Displays login status for a user:

3 Type **/var/adm/loginlog**, then press **Return/Enter**. To enable login Logging, this creates the log file **loginlog**.

4 Type **chmod 600 /var/adm/loginlog,** then press **Return/Enter**. This sets read and write permissions for root on the file.

5 Type **chgrep sys /var/adm/loginlog,** then press **Return/Enter**. This sets the group to **sys**.

Monitoring and Reviewing User Audit Trail Information

The **audit_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

/etc/security/audit_startup

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the audit_control file and re-initialize the current audit directory to the first directory listed in the audit_control file or to open a new audit file in the current audit directory specified in the audit_control file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

Audit Commands Procedures

1 **audit -n**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

2 **audit -s**, then press **Return/Enter**.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

3 **audit -t**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file, disable audit and die.

4 **praudit -sl *filename***, then press **Return/Enter**.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file /usr/include/sys/audit.h. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.

Practical Exercises

Introduction

These practical exercises are presented in "day-in-the-life" scenarios relating to system administration activities. They represent real situations that you, as System Administrator, are likely to encounter on a day-to-day basis.

Equipment and Materials

A functioning ECS computer system.

System Startup and Shutdown

The EOSDIS system was taken down for maintenance earlier in the day and the maintenance has been completed. You must now bring the system to full operation. Turn on the entire ECS system in the prescribed order.

-or-

Startup the following servers:

- SQL Server
- *server 2*
- *server 3*

Tape Operations, System Backup and Restore

1 You have received an approved request from the SEO Chief to perform an incremental backup of the SQL Server for files created or modified within the past 48 hours.

2 Determine how many tapes it will take to back up the required data.

3 Prepare the appropriate number of new tapes to accommodate the backup and perform the label and inventory operations on the tapes.

4 Perform the incremental backup.

5 Inform the SEO Chief that the backup has been performed.

6 ***xuser*** calls you and tells you that she has inadvertently erased the following three files that are critical to her research:

- file1
- file2
- file3

7 She does not remember exactly when they are were last modified. Locate the latest versions of each of the files and perform a file restoration.

User Administration

1 Add the individual to the system(Figure 54):

UNIX User Registration Request

REQUESTER INFORMATION:

Name: **Erica J. Sonnenshein**

Office Phone Number: **(301) 999-5555**

E-Mail Address: **esonnens@gsfc.nasa.gov** Office Location: **Bldg. 32**

NEW USER INFORMATION:

Name: **Peter Kovalkaides**

Office Phone Number: **(301) 555-1234**

Home Phone Number: **(301) 444-4444**

Organization: **GSFC DAAC**

Group Affiliation(s): **SMC**

Role(s)/Job(s)/Justification: **computer operator with database access required**

Date of Request: **9/17/97** Date Required: **9/22/97**

Supervisor Approval: _____ Date: _____

Ops Supervisor Approval: _____ Date: _____

Figure 39. UNIX User Registration Request Form.

2 The user you just added has called you with the news that he has forgotten his password. Describe the procedures you must follow to receive authorization to change the individual's password. Assuming you have received the appropriate authorizations, change the password to gnu-Uzr.

3 Change the group affiliations for this user to ***new-group affiliation.***

4 Peter Kovalkaides sends you an e-mail message informing that the work on his task is complete and requests that you change the access privileges on all files owned by him to READ ONLY for all classes of users to protect the files from changes.

5 You have determined that space on the ***xserver*** is becoming rather scarce. There are a few large files (***insert-file-names-here***) that need to be deleted, and since ***xuser*** and Peter Kovalkaides are done with their projects, their home directories need to be moved to ***insert-new-location-here***. Perform the procedures that will accomplish these tasks assuming you have received the appropriate authorizations. When you are done, inform the affected users of the changes.

System Log Maintenance

1 The icon on the ECS Desktop for the SQL Server has turned red. Check the system log to find out what the problem is.

2 The problem in the exercise in this exercise requires you to restart the SQL server without affecting any of the other subsystems. Perform this task now.

This page intentionally left blank.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

This page intentionally left blank.